Appendix A
Answers to Review Questions

Chapter 1: Security Governance Through Principles and Policies

1. C. Hardware destruction is a violation of availability and possibly integrity. Violations of confidentiality include stealing passwords, eavesdropping, and social engineering.
2. B. The primary goals and objectives of security are confidentiality, integrity, and availability, commonly referred to as the CIA Triad. The other options are incorrect. A security infrastructure needs to establish a network's border perimeter security, but that is not a primary goal or objective of security. AAA services are a common component of secured systems, which can provide support for accounting, but the primary goals of security remain the elements of the CIA Triad. Ensuring that subject activities are recorded is the purpose of auditing, but that is not a primary goal or objective of security.
3. B. Availability means that authorized subjects are granted timely and uninterrupted access to objects. Identification is claiming an identity, the first step of AAA services. Encryption is protecting the confidentiality of data by converting plaintext into ciphertext. Layering is the use of multiple security mechanisms in series.
4. D. Security governance seeks to compare the security processes and infrastructure used within the organization with knowledge and insight obtained from external sources. The other statements are not related to security governance.
5. C. A strategic plan is a long-term plan that is fairly stable. It defines the organization's security purpose. It defines the security function and aligns it with the goals, mission, and objectives of the organization. The tactical plan is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan or can be crafted ad hoc based on unpredicted events. An operational plan is a short-term, highly detailed plan based on strategic and tactical plans. It is valid or useful only for a short time. A rollback plan is a

means to return to a prior state after a change does not meet expectations.

6. A, C, D, F. Acquisitions and mergers place an organization at an increased level of risk. Such risks include inappropriate information disclosure, data loss, downtime, and failure to achieve a sufficient return on investment (ROI). Increased worker compliance is not a risk, but a desired security precaution against the risks of acquisitions. Additional insight into the motivations of inside attackers is not a risk, but a potential result of investigating breaches or incidents related to acquisitions.
7. C. Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards and requirements designed to ensure the protection of sensitive credit card and debit card information. The other options are incorrect. Information Technology Infrastructure Library (ITIL) was initially crafted by the British government for domestic use but is now an international standard, which is a set of recommended best practices for core IT security and operational processes, and is often used as a starting point for the crafting of a customized IT security solution. ISO 27000 is a family group of international security standards that can be the basis for implementing organizational security and related management practices. NIST Cybersecurity Framework (CSF) is designed for critical infrastructure and commercial organizations and consists of five functions: Identify, Protect, Detect, Respond, and Recover. It is a prescription of operational activities that are to be performed on an ongoing basis for the support and improvement of security over time.
8. B. The security professional has the functional responsibility for security, including writing the security policy and implementing it. Senior management is ultimately responsible for the security maintained by an organization and should be most concerned about the protection of its assets. The custodian role is assigned to the person who is responsible for the tasks of implementing the prescribed protection defined by the security policy and senior management. An auditor is responsible for reviewing and

verifying that the security policy is properly implemented and that the derived security solutions are adequate.

9. A, B, C, E. The COBIT key principles are: Provide Stakeholder Value (C), Holistic Approach (A), Dynamic Governance System (E), Governance Distinct from Management (not listed), Tailored to Enterprise Needs (not listed), and End-to-End Governance System (B). The concept of maintaining authenticity and accountability are good security ideas, but not a COBIT key principle.

10. A, D. Due diligence is establishing a plan, policy, and process to protect the interests of an organization. Due care is practicing the individual activities that maintain the security effort. The other options are incorrect; they have the terms inverted. The corrected statements are as follows: Due diligence is developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures. Due care is the continued application of a security structure onto the IT infrastructure of an organization. Due diligence is knowing what should be done and planning for it. Due care is doing the right action at the right time.

11. B. A policy is a document that defines the scope of security needed by the organization and discusses the assets that require protection and the extent to which security solutions should go to provide the necessary protection. A standard defines compulsory requirements for the homogenous use of hardware, software, technology, and security controls. A procedure is a detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution. A guideline offers recommendations on how security requirements are implemented and serves as an operational guide for both security professionals and users. III is the definition of a baseline, which was not included as a component option.

12. D. When confidential documents are exposed to unauthorized entities, this is described by the I in STRIDE, which represents information disclosure. The elements of STRIDE are spoofing,

tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

13. B. This scenario describes a proactive approach to threat modeling, which is also known as the defensive approach. A reactive approach or adversarial approach to threat modeling takes place after a product has been created and deployed. There is no threat modeling concept known as the qualitative approach. Qualitative is typically associated with a form of risk assessment.

14. A, B, D. These statements are true: (A) Each link in the supply chain should be responsible and accountable to the next link in the chain; (B) Commodity vendors are unlikely to have mined their own metals, processed the oil for plastics, or etched the silicon of their chips; and (D) Failing to properly secure a supply chain can result in flawed or less reliable products, or even embedded listing or remote control mechanisms. The remaining option is incorrect. Even if a final product seems reasonable and performs all necessary functions, that does not provide assurance that it is secure or that it was not tampered with somewhere in the supply chain.

15. D. Though not explicitly stating hardware, this scenario describes a typical and potential risk of a supply chain, that a hardware risk results in the presence of a listening mechanism in the final product. This scenario does not provide information that would indicate that the supply chain risk is focused on software, services, or data.

16. B. In this scenario, Cathy should void the authorization to operate (ATO) of this vendor. This situation describes the fact that the vendor is not meeting minimal security requirements, which are necessary for the protection of the service and its customers. Writing a report is not a sufficient response to this discovery. You may have assumed Cathy does or does not have the authority to perform any of the other options, but there is no indication of Cathy's position in the organization. It is reasonable for a CEO to ask the CISO to perform such an evaluation. Regardless, the report should be submitted to the CISO, not the CIO, whose focus is primarily on ensuring that

information is used effectively to accomplish business objectives, not that such use is secure. Reviewing terms and conditions will not make any difference in this scenario, as those typically apply to customers, not internal operations. Reviewing does not necessarily cause a change or improvement to insecure practices. A vendor-signed NDA has no bearing on this scenario.

17. A. Minimum security requirements should be modeled on your existing security policy. This is based on the idea that when working with a third party, that third party should have at least the same security as your organization. A third-party audit is when a third-party auditor is brought in to perform an unbiased review of an entity's security infrastructure. This audit may reveal where there are problems, but the audit should not be the basis of minimum security requirements for a third party. On-site assessment is when you visit the site of the organization to interview personnel and observe their operating habits. This is not the basis for establishing minimum security requirements for a third party. Vulnerability scan results, like third-party audits, may reveal concerns, but it is not the basis for establishing minimum security requirements for a third party.

18. C. Process for Attack Simulation and Threat Analysis (PASTA) is a seven-stage threat modeling methodology. PASTA is a risk-centric approach that aims at selecting or developing countermeasures in relation to the value of the assets to be protected. Visual, Agile, and Simple Threat (VAST) is a threat modeling concept that integrates threat and risk management into an Agile programming environment on a scalable basis. DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) is a flexible threat rating system that is based on the answers to five main questions about a threat. STRIDE is a threat categorization scheme developed by Microsoft.

19. B, C, E, F, G. The five key concepts of decomposition are trust boundaries, dataflow paths, input points, privileged operations, and details about security stance and approach. Patch or update version management is an important part of security management in general; it is just not a specific component of

decomposition. Determining open- versus closed-source code use is not an element of decomposition.

20. A, B, C, D, E, F, G, H, I. All of the listed options are terms that relate to or are based on defense in depth: layering, classifications, zones, realms, compartments, silos, segmentations, lattice structure, and protection rings.

Chapter 2: Personnel Security and Risk Management Concepts

1. D. Regardless of the specifics of a security solution, humans are often considered the weakest element. No matter what physical or logical controls are deployed, humans can discover ways to avoid them, circumvent or subvert them, or disable them. Thus, it is important to take into account the humanity of your users when designing and deploying security solutions for your environment. Software products, internet connections, and security policies can all be vulnerabilities or otherwise areas of security concern, but they are not considered the most common weakest element of an organization.
2. A. The first step in hiring new employees is to create a job description. Without a job description, there is no consensus on what type of individual needs to be found and hired. Crafting job descriptions is the first step in defining security needs related to personnel and being able to seek out new hires. From the job description, a determination can be made as to the education, skills, experience, and classification required by the applicant. Then a job posting can be made to request the submission of résumés. Then, candidates can be screened to see if they meet the requirements and if they have any disqualifications.
3. B. Onboarding is the process of adding new employees to the organization, having them review and sign policies, be introduced to managers and coworkers, and be trained in employee operations and logistics. Reissue is a certification function when a lost certificate is provided to the user by extracting it from the escrow backup database or when a certificate is altered to extend its expiration date. Background checks are used to verify that a job applicant is qualified but not disqualified for a specific work position. A site survey is used to optimize the placement of wireless access points (WAPs) to provide reliable connectivity throughout the organization's facilities.

4. B. A termination process often focuses on eliminating an employee who has become problematic, whether that employee is committing crimes or just violating company policy. Once the worker is fired, the company has little direct control over that person. So, the only remaining leverage is legal, which often relates to a nondisclosure agreement (NDA). Hopefully, reviewing and reminding the former employee about their signed NDA will reduce future security issues, such as confidential data dissemination. Returning the exiting employee's personal belongings is not really an important task to protect the company's security interests. Evaluating the exiting employee's performance could be done via an exit interview, but that was not mentioned in this scenario. Often when an adversarial termination occurs, an exit interview is not feasible. Canceling an exiting employee's parking permit is not a high security priority for most organizations, at least not in comparison to the NDA.
5. C. Option C is correct: Multiparty risk exists when several entities or organizations are involved in a project. The risk or threats are often due to the variations of objectives, expectations, timelines, budgets, and security priorities of those involved. The other statements are false. Their corrected and thus true versions would be: (A) using service- level agreements (SLAs) is a means to ensure that organizations providing services maintain an appropriate level of service agreed on by the service provider, vendor, or contractor and the customer organization; (B) outsourcing can be used as a risk response option known as transference or assignment; and (D) risk management strategies implemented by one party may in fact cause additional risks to or from another party.
6. A. An asset is anything used in a business process or task. A threat is any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset. A vulnerability is the weakness in an asset, or the absence or the weakness of a safeguard or countermeasure. An exposure is being susceptible to asset loss because of a threat; there is the possibility that a vulnerability can or will be exploited. Risk is the possibility or likelihood that a threat will exploit a

vulnerability to cause harm to an asset and the severity of damage that could result.

7. B. The threat of a fire and the vulnerability of a lack of fire extinguishers lead to the risk of damage to equipment. This scenario does not relate to virus infection or unauthorized access. Equipment damaged by fire could be considered a system malfunction, but that option is not as direct as “damage to equipment.”
8. D. This scenario is describing the activity of performing a quantitative risk assessment. The question describes the determination of asset value (AV) as well as the exposure factor (EF) and the annualized rate of occurrence (ARO) for each identified threat. These are the needed values to calculate the annualized loss expectancy (ALE), which is a quantitative factor. This is not an example of a qualitative risk assessment, since specific numbers are being determined rather than relying on ideas, reactions, feelings, and perspectives. This is not the Delphi technique, which is a qualitative risk assessment method that seeks to reach an anonymous consensus. This is not risk avoidance, since that is an optional risk response or treatment, and this scenario is only describing the process of risk assessment.
9. C. The annual costs of safeguards should not exceed the expected annual cost of asset value loss. The other statements are not rules to follow. (A) The annual cost of the safeguard should not exceed the annual cost of the asset value or its potential value loss. (B) The cost of the safeguard should be less than the value of the asset. (D) There is no specific maximum percentage of a security budget for the cost of a safeguard. However, the security budget should be used efficiently to reduce overall risk to an acceptable level.
10. C. When controls are not cost effective, they are not worth implementing. Thus, risk acceptance is the risk response in this situation. Mitigation is the application of a control; that was not done in this scenario. Ignoring risk occurs when no action, not even assessment or control evaluation, is performed in relation to a risk. Since controls were evaluated in this scenario, this is

not ignoring risk. Assignment is the transfer of risk to a third party; that was not done in this scenario.

11. A. The value of a safeguard to an organization is calculated by ALE before safeguard – ALE after implementing the safeguard – annual cost of safeguard [(ALE1 – ALE2) – ACS]. This is known as the cost/benefit equation for safeguards. The other options are incorrect. (B) This is an invalid calculation. (C) This is an invalid calculation. (D) This is the concept formula for residual risk: total risk – controls gap = residual risk.

12. A, C. Statements of A and C are valid definitions of risk. The other two statements are not definitions of risk. (B) Anything that removes a vulnerability or protects against one or more specific threats is considered a safeguard or a countermeasure, not a risk. (D) The presence of a vulnerability when a related threat exists is an exposure, not a risk. A risk is a calculation of the probability of occurrence and the level of damage that could be caused if an exposure is realized (i.e., actually occurs).

13. A. This situation is describing inherent risk. Inherent risk is the level of natural, native, or default risk that exists in an environment, system, or product prior to any risk management efforts being performed. The new application had vulnerabilities that were not mitigated, thus enabling the opportunity for the attack. This is not a risk matrix. A risk matrix or risk heat map is a form of risk assessment that is performed on a basic graph or chart, such as a 3×3 grid comparing probability and damage potential. This is not a qualitative risk assessment, since this scenario does not describe any evaluation of the risk of the new code. This is not residual risk, since no controls were implemented to reduce risk. Residual risk is the leftover risk after countermeasures and safeguards are implemented in response to original or total risk.

14. C. The level of RMM named Defined requires that a common or standardized risk framework be adopted organization-wide. This is effectively level 3. The first level of RMM is not listed as an option; it is ad hoc, which is the chaotic starting point. Preliminary is RMM level 2, which demonstrates loose attempts to follow risk management processes, but each department may

perform risk assessment uniquely. Integrated is RMM level 4, where risk management operations are integrated into business processes, metrics are used to gather effectiveness data, and risk is considered an element in business strategy decisions. Optimized is RMM level 5, where risk management focuses on achieving objectives rather than just reacting to external threats, increasing strategic planning toward business success rather than just avoiding incidents, and reintegrating lessons learned into the risk management process.

15. B. The RMF phase 6 is Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable. The phases of RMF are (1) Prepare, (2) Categorize, (3) Select, (4) Implement, (5) Assess, (6) Authorize, and (7) Monitor. (A) RMF phase (2) is categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss. (C) RMF phase (5) is assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements. (D) RMF phase (7) is monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

16. B, F. The leaking of company proprietary data may have been caused by the content of emails received by workers. The computers of workers who clicked links from the suspicious emails may have been infected by malicious code. This malicious code may have exfiltrated documents to the social media site. This issue could occur whether workers were on company computers on the company network, on company computers on their home network, or on personal computers on their home network (especially if the workers copied company files to their personal machines to work from home). Blocking access to social media sites and personal email services from the company network reduces the risk of this same event occurring again. For

example, if the suspicious emails are blocked from being received by company email servers and accounts, they could still be received into personal email accounts. Though not mentioned, blocking access to the malicious URLs would be a good security defense as well. This issue is not addressed by deploying a web application firewall, updating the company email server, using MFA on the email server, or performing an access review of company files. Although all of these options are good security practices in general, they do not relate specifically to this issue.

17. C. Training is teaching employees to perform their work tasks and to comply with the security policy. Training is typically hosted by an organization and is targeted to groups of employees with similar job functions. (A) Education is an endeavor in which students and users learn much more than they actually need to know to perform their work tasks. Education is most often associated with users pursuing certification or seeking job promotion or career advancement. Most education programs are not hosted by the employer but by training organizations or colleges or universities. Education is not provided to workers in groups based on their job positions. (B) Awareness establishes a common baseline or foundation of security understanding across the entire organization and focuses on key or basic topics and issues related to security that all employees must understand. Although it is provided by the organization, it is not targeted to groups of workers since it applies to all employees. (D) Termination is usually targeted at individuals rather than groups of workers with similar job positions. Though large layoff events might fire groups of similar workers, this option is not as accurate as training.
18. B, C, D. The activity described in option A is an opportunistic unauthorized access attack, which is not a social engineering attack since there was no interaction with the victim, just the opportunity when the victim walked away. The activities described in options B (hoax), C (phishing, hoax, watering hole attack), and D (vishing) are all examples of social engineering attacks.

19. B. The correct answer for these blanks is security champion(s). Often a security champion is a member of a group who decides (or is assigned) to take charge of leading the adoption and integration of security concepts into the group's work activities. Security champions are often non-security employees who take up the mantle to encourage others to support and adopt more security practices and behaviors. The other options are incorrect. A CISO, or chief information security officer, defines and enforces security throughout the organization. The security auditor is the person who manages security logging and reviews the audit trails for signs of compliance or violation. The custodian is the security role that accepts assets from owners and then, based on the owner-assigned classifications, places the asset in the proper IT container where the proper security protections are provided.
20. D. Security awareness and training can often be improved through gamification. Gamification is a means to encourage compliance and engagement by integrating common elements of gameplay into other activities, such as security compliance and behavior change. This can include rewarding compliance behaviors and potentially punishing violating behaviors. Many aspects of gameplay can be integrated into security training and adoption, such as scoring points, earning achievements or badges (i.e., earning recognition), competing with others, cooperating with others (i.e., teaming up with coworkers), following a set of common/standard rules, having a defined goal, seeking rewards, developing group stories/experiences, and avoiding pitfalls or negative game events. (A) Program effectiveness evaluation is using some means of verification, such as giving a quiz or monitoring security incident rate changes over time, to measure whether the training is beneficial or a waste of time and resources. This question starts by indicating that security incidents are on the rise, which shows that prior training was ineffective. But the recommendations to change the training are gamification-focused. (B) Onboarding is the process of adding new employees to the organization. This is not the concept being described in this scenario. (C) Compliance enforcement is the application of sanctions or consequences for

failing to follow policy, training, best practices, and/or regulations.

Chapter 3: Business Continuity Planning

1. B. As the first step of the process, the business organization analysis helps guide the remainder of the work. James and his core team should conduct this analysis and use the results to aid in the selection of team members and the design of the BCP process.
2. C. This question requires that you exercise some judgment, something that is extremely important for CISSP candidates. All of these answers are plausible things that Tracy could bring up, but we're looking for the best answer. In this case, that is ensuring that the organization is ready for an emergency—a mission-critical goal. Telling managers that the exercise is already scheduled or required by policy doesn't address their concerns that it is a waste of time. Telling them that it won't be time-consuming is not likely to be an effective argument because they are already raising concerns about the amount of time requested.
3. C. A firm's officers and directors are legally bound to exercise due diligence in conducting their activities. This concept creates a fiduciary responsibility on their part to ensure that adequate business continuity plans are in place. This is an element of corporate responsibility, but that term is vague and not commonly used to describe a board's responsibilities. Disaster requirement and going concern responsibilities are also not risk management terms.
4. D. During the planning phase, the most significant resource utilization will be the time dedicated by members of the BCP team to the planning process. This represents a significant use of business resources and is another reason that buy-in from senior management is essential.
5. A. The quantitative portion of the priority identification should assign asset values in monetary units. The organization may also choose to assign other values to assets, but non-monetary

measures should be part of a qualitative, rather than a quantitative, assessment.

6. C. The annualized loss expectancy (ALE) represents the amount of money a business expects to lose to a given risk each year. This figure is quite useful when performing a quantitative prioritization of business continuity resource allocation.
7. C. The maximum tolerable downtime (MTD) represents the longest period a business function can be unavailable before causing irreparable harm to the business. This figure is useful when determining the level of business continuity resources to assign to a particular function.
8. B. The single loss expectancy (SLE) is the product of the asset value (AV) and the exposure factor (EF). From the scenario, you know that the AV is $3 million and the EF is 90 percent, based on that the same land can be used to rebuild the facility. This yields an SLE of $2,700,000.
9. D. This problem requires you to compute the annualized loss expectancy (ALE), which is the product of the single loss expectancy (SLE) and the annualized rate of occurrence (ARO). From the scenario, you know that the ARO is 0.05 (or 5 percent). From question 8, you know that the SLE is $2,700,000. This yields an ALE of $135,000.
10. A. This problem requires you to compute the ALE, which is the product of the SLE and ARO. From the scenario, you know that the ARO is 0.10 (or 10 percent). From the scenario presented, you know that the SLE is $7.5 million. This yields an ALE of $750,000.
11. C. Risk mitigation controls to address acceptable risks would not be in the BCP. The risk acceptance documentation should contain a thorough review of the risks facing the organization, including the determination as to which risks should be considered acceptable and unacceptable. For acceptable risks, the documentation should include a rationale for that decision and a list of potential future events that might warrant a reconsideration of that determination. The documentation should include a list of controls used to mitigate unacceptable

risks, but it would not include controls used to mitigate acceptable risks, since acceptable risks do not require mitigation.

12. D. The safety of human life must always be the paramount concern in business continuity planning. Be sure that your plan reflects this priority, especially in the written documentation that is disseminated to your organization's employees!
13. C. It is difficult to put a dollar figure on the business lost because of negative publicity. Therefore, this type of concern is better evaluated through a qualitative analysis. The other items listed here are all more easily quantifiable.
14. B. The single loss expectancy (SLE) is the amount of damage that would be caused by a single occurrence of the risk. In this case, the SLE is $10 million, the expected damage from one tornado. The fact that a tornado occurs only once every 100 years is not reflected in the SLE but would be reflected in the annualized loss expectancy (ALE).
15. C. The annualized loss expectancy (ALE) is computed by taking the product of the single loss expectancy (SLE), which was $10 million in this scenario, and the annualized rate of occurrence (ARO), which was 0.01 in this example. These figures yield an ALE of $100,000.
16. C. In the provisions and processes subtask, the BCP team designs the procedures and mechanisms to mitigate risks that were deemed unacceptable during the strategy development phase.
17. D. This is an example of alternative systems. Redundant communications circuits provide backup links that may be used when the primary circuits are unavailable.
18. C. Disaster recovery plans pick up where business continuity plans leave off. After a disaster strikes and the business is interrupted, the disaster recovery plan guides response teams in their efforts to quickly restore business operations to normal levels.

19. A. The annualized rate of occurrence (ARO) is the likelihood that the risk will materialize in any given year. The fact that a power outage did not occur in any of the past three years doesn't change the probability that one will occur in the upcoming year. Unless other circumstances have changed, the ARO should remain the same.
20. C. You should strive to have the highest-ranking person possible sign the BCP's statement of importance. Of the choices given, the chief executive officer (CEO) is the highest ranking.

Chapter 4: Laws, Regulations, and Compliance

1. C. The Bureau of Industry and Security within the Department of Commerce sets regulations on the export of encryption products outside of the United States. The other agencies listed here are not involved in regulating exports.
2. A. The Federal Information Security Management Act (FISMA) includes provisions regulating information security at federal agencies. It places authority for classified systems in the hands of the National Security Agency (NSA) and authority for all other systems with the National Institute for Standards and Technology (NIST).
3. D. Administrative laws do not require an act of the legislative branch to implement at the federal level. Administrative laws consist of the policies, procedures, and regulations promulgated by agencies of the executive branch of government. Although they do not require an act of Congress, these laws are subject to judicial review and must comply with criminal and civil laws enacted by the legislative branch.
4. A. The California Consumer Privacy Act (CCPA) of 2018 was the first sweeping data privacy law enacted by a U.S. state. This follows California's passing of the first data breach notification law, which was modeled after the requirements of the European Union's General Data Protection Regulation (GDPR).
5. B. The Communications Assistance for Law Enforcement Act (CALEA) required that communications carriers assist law enforcement with the implementation of wiretaps when done under an appropriate court order. CALEA only applies to communications carriers and does not apply to financial institutions, healthcare organizations, or websites.
6. B. The Fourth Amendment to the U.S. Constitution sets the “probable cause” standard that law enforcement officers must follow when conducting searches and/or seizures of private

property. It also states that those officers must obtain a warrant before gaining involuntary access to such property. The Privacy Act regulates what information government agencies may collect and maintain about individuals. The Second Amendment grants the right to keep and bear arms. The Gramm–Leach–Bliley Act regulates financial institutions, not the federal government.

7. A. Copyright law is the only type of intellectual property protection available to Matthew. It covers only the specific software code that Matthew used. It does not cover the process or ideas behind the software. Trademark protection is not appropriate for this type of situation because it would only protect the name and/or logo of the software, not its algorithms. Patent protection does not apply to mathematical algorithms. Matthew can't seek trade secret protection because he plans to publish the algorithm in a public technical journal.
8. D. Mary and Joe should treat their oil formula as a trade secret. As long as they do not publicly disclose the formula, they can keep it a company secret indefinitely. Copyright and patent protection both have expiration dates and would not meet Mary and Joe's requirements. Trademark protection is for names and logos and would not be appropriate in this case.
9. C. Richard's product name should be protected under trademark law. Until his registration is granted, he can use the ™ symbol next to it to inform others that it is protected under trademark law. Once his application is approved, the name becomes a registered trademark, and Richard can begin using the ® symbol. The © symbol is used to represent a copyright. The † symbol is not associated with intellectual property protections.
10. A. The Privacy Act of 1974 limits the ways government agencies may use information that private citizens disclose to them under certain circumstances. The Electronic Communications Privacy Act (ECPA) implements safeguards against electronic eavesdropping. The Health Insurance Portability and Accountability Act (HIPAA) regulates the protection and sharing of health records. The Gramm–Leach–Bliley Act requires that financial institutions protect customer records.

11. D. The European Union provides standard contractual clauses that may be used to facilitate data transfer. That would be the best choice in a case where two different companies are sharing data. If the data were being shared internally within a company, binding corporate rules would also be an option. The EU/US Privacy Shield was a safe harbor agreement that would previously have allowed the transfer but that is no longer valid. Privacy Lock is a made-up term.
12. A. The Children's Online Privacy Protection Act (COPPA) provides severe penalties for companies that collect information from young children without parental consent. COPPA states that this consent must be obtained from the parents of children younger than the age of 13 before any information is collected (other than basic information required to obtain that consent).
13. D. Although state data breach notification laws vary, they generally apply to Social Security numbers, driver's license numbers, state identification card numbers, credit/debit card numbers, and bank account numbers. These laws generally do not cover other identifiers, such as a student identification number.
14. B. Organizations subject to HIPAA may enter into relationships with service providers as long as the provider's use of protected health information is regulated under a formal business associate agreement (BAA). The BAA makes the service provider liable under HIPAA.
15. B. Cloud services almost always include binding click-through license agreements that the user may have agreed to when signing up for the service. If that is the case, the user may have bound the organization to the terms of that agreement. This agreement does not need to be in writing. There is no indication that the user violated any laws.
16. B. The Gramm–Leach–Bliley Act (GLBA) provides, among other things, regulations regarding the way financial institutions can handle private information belonging to their customers.
17. C. U.S. patent law provides for an exclusivity period of 20 years beginning at the time a utility patent application is submitted to

the Patent and Trademark Office.

18. C. Ryan does not likely need to be concerned about HIPAA compliance because that law applies to healthcare organizations and Ryan works for a financial institution. Instead, he should be more concerned about compliance with the Gramm–Leach–Bliley Act (GLBA). The other concerns should all be part of Ryan's contract review.
19. C. The Payment Card Industry Data Security Standard (PCI DSS) applies to organizations involved in storing, transmitting, and processing credit card information.
20. D. Copyright protection generally lasts for 70 years after the death of the last surviving author of the work.

Chapter 5: Protecting Security of Assets

1. B. Data classifications provide strong protection against the loss of confidentiality and are the best choice of the available answers. Data labels and proper data handling are based on first identifying data classifications. Data degaussing methods apply only to magnetic media.
2. D. Backup media should be protected with the same level of protection afforded the data it contains, and using a secure off-site storage facility would ensure this. The media should be marked, but that won't protect it if it is stored in an unstaffed warehouse. A copy of backups should be stored off-site to ensure availability if a catastrophe affects the primary location. If copies of data are not stored off-site or off-site backups are destroyed, security is sacrificed by risking availability.
3. B. Destruction is the final stage in the life cycle of backup media. Because the backup method is no longer using tapes, they should be destroyed. Degaussing and declassifying the tape is done if you plan to reuse it. Retention implies you plan to keep the media, but retention is not needed at the end of its life cycle.
4. C. The data owner is the person responsible for classifying data. A data controller decides what data to process and directs the data processor to process the data. A data custodian protects the integrity and security of the data by performing day-to-day maintenance. Users simply access the data.
5. A. The data custodian is responsible for the tasks of implementing the protections defined by the security policy and senior management. A data controller decides what data to process and how. Data users are not responsible for implementing the security policy protections. Data processors control the processing of data and only do what the data controller tells them to do with the data.
6. D. The company can implement a data collection policy of minimization to minimize the amount of data they collect and store. If they are selling digital products, they don't need the

physical address. If they are reselling products to the same customers, they can use tokenization to save tokens that match the credit card data, instead of saving and storing credit card data. Anonymization techniques remove all personal data and make the data unusable for reuse on the website. Pseudonymization replaces data with pseudonyms or artificial identifiers. Although the process can be reversed, it is not necessary.

7. B. Security labeling identifies the classification of data such as sensitive, secret, and so on. Media holding sensitive data should be labeled. Similarly, systems that hold or process sensitive data should also be labeled. Many organizations require the labeling of all systems and media, including those that hold or process nonsensitive data.
8. B. A data subject is a person that can be identified by an identifier such as a name, identification number, or other PII. All of these answers refer to the General Data Protection Regulation (GDPR). A data owner owns the data and has ultimate responsibility for protecting it. A data controller decides what data to process, the purpose of collecting data, and how it should be processed. A data processor processes the data for the data controller.
9. B. Personnel did not follow the record retention policy for the backups sent to the warehouse. The scenario states that administrators purge on-site emails older than six months to comply with the organization's security policy, but the leak was from emails sent over three years ago. Personnel should follow media destruction policies when the organization no longer needs the media, but the issue here is the data on the tapes. Configuration management ensures that systems are configured correctly using a baseline, but this does not apply to backup media. Versioning applies to applications, not backup tapes.
10. D. Record retention policies define the amount of time to keep data, and laws or regulations often drive these policies. Data remanence is data remnants on media, and proper data destruction procedures remove data remnants. Laws and

regulations do outline requirements for some data roles, but they don't specify requirements for the data user role.

11. D. Purging is the most reliable method of the given choices. Purging overwrites the media with random bits multiple times and includes additional steps to ensure that data is removed. It ensures there isn't any data remanence. Erasing or deleting processes rarely remove the data from media but instead mark it for deletion. Solid-state drives (SSDs) do not have magnetic flux, so degaussing an SSD doesn't destroy data.
12. A. Overwriting the disks multiple times will remove existing data. This is called purging, and purged media can then be used again. Formatting the disks isn't secure because it doesn't typically remove the previously stored data. Deleting the files removes them from the directory but leaves remanent data on the disk that may be recovered with forensic tools. Defragmenting a disk optimizes it, but it doesn't remove data.
13. D. Systems with an EOS date that occurs in the following year should be a top priority for replacement. The EOS date is the date that the vendor will stop supporting a product. The EOL date is the date that a vendor stops producing and offering a product for sales but the vendor continues to support the product until the EOS date. Systems used for data loss prevention or to process sensitive data can remain in service.
14. D. Purging memory buffers remove all remnants of data after a program has used it. Asymmetric encryption (along with symmetric encryption) protects data in transit or at rest. The data is already encrypted and stored in the database. Data loss prevention methods prevent unauthorized data loss but do not protect data in use.
15. A. Symmetric encryption methods protect data at rest, and data at rest is any data stored on media such as a server. Data in transit is data being transferred between two systems. Data in use is data in memory that is used by an application. Steps are taken to protect data from the time it is created to the time it is destroyed, but this question isn't related to the data life cycle.

16. B. Scoping is a part of the tailoring process and refers to reviewing a list of security and privacy controls and selecting the controls that apply. Tokenization is the use of a token, such as a random string of characters, to replace other data and is unrelated to this question. Note that scoping focuses on the security of the system, and tailoring ensures that the selected controls align with the organization's mission. If the database server needs to comply with external entities, it's appropriate to select a standard baseline provided by that entity. Imaging is done to deploy an identical configuration to multiple systems, but this is typically done after identifying security controls.
17. A. Tailoring refers to modifying a list of security controls to align with the organization's mission. The IT administrators identified a list of security controls to protect the web farm during the scoping steps. Sanitization methods (such as purging and destroying) help ensure that data cannot be recovered and is unrelated to this question. Asset classification identifies the classification of assets based on the classification of data the assets hold or process. Minimization refers to data collection. Organizations should collect and maintain only the data they need.
18. A. A cloud access security broker (CASB) is a software solution placed logically between users and cloud-based resources, and it can enforce security policies used in an internal network. Data loss prevention (DLP) systems attempt to detect and block data exfiltration. CASB systems typically include DLP capabilities. Digital rights management (DRM) methods attempt to provide copyright protection for copyrighted works. End of life (EOL) is generally a marketing term and indicates when a company stops producing and selling a product.
19. B. Network-based data loss prevention (DLP) systems can scan outgoing data and look for specific keywords and/or data patterns. DLP systems can block these outgoing transmissions. Antimalware software detects malware. Security information and event management (SIEM) provides real-time analysis of events occurring on systems throughout an organization but doesn't necessarily scan outgoing traffic. Intrusion prevention

systems (IPSs) scan incoming traffic to prevent unauthorized intrusions.

20. B, C, D. Persistent online authentication, automatic expiration, and a continuous audit trail are all methods used with digital rights management (DRM) technologies. Virtual licensing isn't a valid term within DRM.

Chapter 6: Cryptography and Symmetric Key Algorithms

1. A, D. Keys must be long enough to withstand attack for as long as the data is expected to remain sensitive. They should not be generated in a predictable way but, rather, should be randomly generated. Keys should be securely destroyed when they are no longer needed and not indefinitely retained. Longer keys do indeed provide greater security against brute-force attacks.
2. A. Nonrepudiation prevents the sender of a message from later denying that they sent it. Confidentiality protects the contents of encrypted data from unauthorized disclosure. Integrity protects data from unauthorized modification. Availability is not a goal of cryptography.
3. B. The strongest keys supported by the Advanced Encryption Standard are 256 bits. The valid AES key lengths are 128, 192, and 256 bits.
4. D. The Diffie–Hellman algorithm allows the secure exchange of symmetric encryption keys between two parties over an insecure channel.
5. A. Confusion and diffusion are two principles underlying most cryptosystems. Confusion occurs when the relationship between the plaintext and the key is so complicated that an attacker can't merely continue altering the plaintext and analyzing the resulting ciphertext to determine the key. Diffusion occurs when a change in the plaintext results in multiple changes spread throughout the ciphertext.
6. B. B. Randy is aiming to achieve confidentiality with his AES-based cryptosystem. Confidentiality ensures that sensitive information is accessible only to those authorized to view it, which aligns with Randy's goal of preventing unauthorized access to the information. Nonrepudiation, on the other hand, prevents someone from denying an action, such as sending a message, which is not Randy's focus here. Authentication

verifies the identity of the parties involved, and while important, it's not the primary goal of encrypting data to prevent unauthorized access. Integrity ensures that the data has not been tampered with or altered, which, although crucial, is not the same as protecting the data from being read by unauthorized individuals.

7. D. Assuming that it is used properly, the one-time pad is the only known cryptosystem that is not vulnerable to attacks. All other cryptosystems, including transposition ciphers, substitution ciphers, and even AES, are vulnerable to attack, even if no attack has yet been discovered.
8. B, C, D. The encryption key must be at least as long as the message to be encrypted. This is because each key element is used to encode only one character of the message. The three other facts listed are all characteristics of one-time pad systems.
9. C. In a symmetric cryptosystem, a unique key exists for each pair of users. In this case, every key involving the compromised user must be changed, meaning that the key that the user shared with each of the other 19 users must be changed.
10. C. Block ciphers operate on message “chunks” rather than on individual characters or bits. The other ciphers mentioned are all types of stream ciphers that operate on individual bits or characters of a message.
11. A. Symmetric key cryptography uses a shared secret key. All communicating parties utilize the same key for communication in any direction. Therefore, James only needs to create a single symmetric key to facilitate this communication.
12. B. M of N Control requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks. M of N Control is an example of a split knowledge technique, but not all split knowledge techniques are used for key escrow.
13. A. An initialization vector (IV) is a random bit string (a nonce) that is the same length as the block size that is XORed with the message. IVs are used to create a unique ciphertext every time the same message is encrypted with the same key. Vigenère

ciphers are an example of a substitution cipher technique. Steganography is a technique used to embed hidden messages within a binary file. Stream ciphers are used to encrypt continuous streams of data.

14. B. Galois/Counter Mode (GCM) and Counter with Cipher Block Chaining Message Authentication Code mode (CCM) are the only two modes that provide both confidentiality and data authenticity. Other modes, including Electronic Codebook (ECB), Output Feedback (OFB), and Counter (CTR) provide only confidentiality.
15. D. Data that is stored in memory is being actively used by a system and is considered data in use. Data at rest is data that is stored on nonvolatile media, such as a disk. Data in transit is being actively transferred over a network.
16. B, C. The Advanced Encryption Standard (AES) and Rivest Cipher 6 (RC6) are modern, secure algorithms. The Data Encryption Standard (DES) and Triple DES (3DES) are outdated and no longer considered secure.
17. B. One important consideration when using the Cipher Block Chaining (CBC) mode is that errors propagate—if one block is corrupted during transmission, it becomes impossible to decrypt that block and the next block as well. The other modes listed here do not suffer from this flaw.
18. C. Offline key distribution requires a side channel of trusted communication, such as in-person contact. This can be difficult to arrange when users are geographically separated. Alternatively, the individuals could use the Diffie–Hellman algorithm or another asymmetric/public key encryption technique to exchange a secret key. Key escrow is a method for managing the recovery of lost keys and is not used for key distribution.
19. A. The CAST-256 algorithm is a modern, secure cryptographic algorithm. 3DES, RC4, and SKIPJACK are all outdated algorithms that suffer from significant security issues.
20. C. A separate key is required for each pair of users who want to communicate privately. In a group of six users, this would

require a total of 15 secret keys. You can calculate this value by using the formula (n * (n – 1) / 2). In this case, n = 6, resulting in (6 * 5) / 2 = 15 keys.

Chapter 7: PKI and Cryptographic Applications

1. D. Any change, no matter how minor, to a message will result in a completely different hash value. There is no relationship between the significance of the change in the message to the significance of the change in the hash value.
2. B. Side-channel attacks use information gathered about a system's use of resources, electricity consumption, timing, or other characteristics to contribute to breaking the security of encryption. Brute-force attacks seek to exhaust all possible encryption keys. Known plaintext attacks require access to both plaintext and its corresponding ciphertext. Frequency analysis attacks require access to ciphertext.
3. C. Richard must encrypt the message using Sue's public key so that Sue can decrypt it using her own private key. If he encrypted the message with his own public key, the recipient would need to know Richard's private key to decrypt the message. If he encrypted it with his own private key, any user could decrypt the message using Richard's freely available public key. Richard could not encrypt the message using Sue's private key because he does not have access to it. If he did, any user could decrypt it using Sue's freely available public key.
4. C. The major disadvantage of the ElGamal cryptosystem is that it doubles the length of any message it encrypts. Therefore, a 2,048-bit plaintext message would yield a 4,096-bit ciphertext message when ElGamal is used for the encryption process.
5. A. The elliptic curve cryptosystem requires significantly shorter keys to achieve encryption that would be the same strength as encryption achieved with the RSA encryption algorithm. A 3,072-bit RSA key is cryptographically equivalent to a 256-bit elliptic curve cryptosystem key.
6. B. The SHA-2 hashing algorithm comes in four variants. SHA-224 produces 224-bit digests. SHA-256 produces 256-bit

digests. SHA-384 produces 384-bit digests, and SHA-512 produces 512-bit digests. Of the options presented here, only 512 bits is a valid SHA-2 hash length.

7. D. The Secure Sockets Layer (SSL) protocol is deprecated and no longer considered secure. It should never be used. The Secure Hash Algorithm 3 (SHA-3), Transport Layer Security (TLS) 1.3, and IPSec are all modern, secure protocols and standards.
8. A. Cryptographic salt values are added to the passwords in password files before hashing to defeat rainbow table and dictionary attacks. Double hashing does not provide any added security. Adding encryption to the passwords is challenging, because then the operating system must possess the decryption key. A one-time pad is only appropriate for use in human-to-human communications and would not be practical here.
9. B. Sue would have encrypted the message using Richard's public key. Therefore, Richard needs to use the complementary key in the key pair, his private key, to decrypt the message.
10. B. Richard should encrypt the message digest with his own private key. When Sue receives the message, she will decrypt the digest with Richard's public key and then compute the digest herself. If the two digests match, she can be assured that the message was not altered in transit.
11. C. The FIPS 186-5 Digital Signature Standard allows federal government use of the RSA, Elliptic Curve DSA, or Edwards-Curve DSA in conjunction with the SHA-3 hashing function to produce secure digital signatures.
12. B. X.509 governs digital certificates and the public key infrastructure (PKI). It defines the appropriate content for a digital certificate and the processes used by certificate authorities to generate and revoke certificates.
13. B. Fault injection attacks compromise the integrity of a cryptographic device by causing some type of external fault, such as the application of high-voltage electricity. Implementation attacks rely on flaws in the cryptographic algorithm. Timing attacks measure the length of time consumed

by encryption operations. Chosen ciphertext attacks require access to the algorithm.

14. C. HTTPS uses TCP port 443 for encrypted client/server communications over TLS. Port 22 is used by the Secure Shell (SSH) protocol. Port 80 is used by the unencrypted HTTP protocol. Port 1433 is used for Microsoft SQL Server database connections.
15. A. An attacker without any special access to the system would only be able to perform ciphertext-only attacks. Known plaintext and chosen plaintext attacks require the ability to encrypt data. Fault injection attacks require physical access to the facility.
16. A. Rainbow tables contain precomputed hash values for commonly used passwords and may be used to increase the efficiency of password-cracking attacks.
17. C. The PFX format is most closely associated with Windows systems that store certificates in binary format, whereas the P7B format is used for Windows systems storing files in text format. The PEM format is another text format, and the CCM format does not exist.
18. B. Certificate revocation lists (CRLs) introduce an inherent latency to the certificate expiration process due to the time lag between CRL distributions.
19. D. The Merkle–Hellman Knapsack cryptosystem, which relies on the difficulty of factoring super-increasing sequence, has been broken by cryptanalysts. The Advanced Encryption Standard (AES), RSA, and Elliptic Curve Cryptography all remain secure today.
20. B. SSH-2 adds support for simultaneous shell sessions over a single SSH connection. Both SSH-1 and SSH-2 are capable of supporting multifactor authentication. SSH-2 actually drops support for the IDEA algorithm, whereas both SSH-1 and SSH-2 support 3DES.

Chapter 8: Principles of Security Models, Design, and Capabilities

1. C. A closed system is one that uses largely proprietary or unpublished protocols and standards. Options A and D do not describe any particular systems, and option B describes an open system.
2. D. The most likely reason the attacker was able to gain access to the baby monitor was through exploitation of default configuration. Since there is no mention of the exact means used by the attacker in the question, and there is no discussion of any actions of installation, configuration, or security implementation, the only remaining option is to consider the defaults of the device. This is an unfortunately common issue with any device, but especially with IoT equipment connected to Wi-Fi networks. Unless malware was used in the attack, a malware scanner would not be relevant to this situation. This scenario did not mention malware. This type of attack is possible over any network type and all Wi-Fi frequency options. This scenario did not discuss frequencies or network types. There was no mention of any interaction with the parents, which was not required with a device using its default configuration.
3. B. The Blue Screen of Death (BSoD) stops all processing when a critical failure occurs in Windows. This is an example of a fail-secure approach. The BSoD is not an example of a fail-open approach; a fail-open event would have required the system to continue to operate in spite of the error. A fail-open result would have protected availability, but typically by sacrificing confidentiality and integrity protections. This is not an example of a limit check, which is the verification that input is within a preset range or domain. Object-oriented is a type of programming approach, not a means of handling software failure.
4. C. A constrained process is one that can access only certain memory locations. Allowing a process to run for a limited time is

a time limit or timeout restriction, not a confinement. Allowing a process to run only during certain times of the day is a scheduling limit, not a confinement. A process that controls access to an object is authorization, not confinement.

5. D. Declassification is the process of moving an object into a lower level of classification once it is determined that it no longer justifies being placed at a higher level. Only a trusted subject can perform declassification because this action is a violation of the verbiage of the star property of Bell–LaPadula, but not the spirit or intent, which is to prevent unauthorized disclosure. Perturbation is the use of false or misleading data in a database management system to redirect or thwart information confidentiality attacks. Noninterference is the concept of limiting the actions of a subject at a higher security level so they do not affect the system state or the actions of a subject at a lower security level. If noninterference was being enforced, the writing of a file to a lower level would be prohibited. Aggregation is the act of collecting multiple pieces of nonsensitive or low-value information and combining it or aggregating it to learn sensitive or high-value information.
6. B. An access control matrix assembles ACLs from multiple objects into a single table. The rows of that table are the ACEs of a subject across those objects; thus, they are a capabilities list. Separation of duties is the division of administrative tasks into compartments or silos; it is effectively the application of the principle of least privilege to administrators. Biba is a security model that focuses on integrity protection across security levels. Clark–Wilson is a security model that protects integrity using an access control triplet.
7. C. The trusted computing base (TCB) has a component known as the reference monitor in theory, which becomes the security kernel in implementation. The other options do not have this feature. The information flow model is focused on the control of information movement. The Biba model is focused on protecting integrity across a lattice security structure. The Brewer and Nash model was created to permit access controls to change dynamically based on a user's previous activity.

8. C. The three parts of the Clark–Wilson model's access control relationship (aka access triple) are subject, object, and program (or interface). Input sanitization is not an element of the Clark–Wilson model.
9. C. The TCB is the combination of hardware, software, and controls that work together to enforce a security policy. The other options are incorrect. Hosts on a network that support secure transmissions may be able to support VPN connections, use TLS encryption, or implement some other form of data-in-transit protection mechanism. The operating system kernel, other OS components, and device drivers are located in Rings 0–2 of the protection rings concept, or in the Kernel Mode ring in the variation used by Microsoft Windows (see Chapter 9). The predetermined set or domain (i.e., a list) of objects that a subject can access is an allow list.
10. A, B. Although the most correct answer in the context of this chapter is option B, the imaginary boundary that separates the TCB from the rest of the system, option A, the boundary of the physically secure area surrounding your system, is also a correct answer in the context of physical security. The network where your firewall resides is not a unique concept or term, since a firewall can exist in any network as either a hardware device or a software service. A border firewall could be considered a security perimeter protection device, but that was not a provided option. Any connections to your computer system are just pathways of communication to a system's interface—they are not labeled as a security perimeter.
11. C. The reference monitor validates access to every resource prior to granting the requested access. The other options are incorrect. Option D, the security kernel, is the collection of TCB components that work together to implement the reference monitor functions. In other words, the security kernel is the implementation of the reference monitor concept. Option A, a TCB partition, and option B, a trusted library, are not valid TCB concept components.
12. B. Option B is the only option that correctly defines a security model. The other options are incorrect. Option A is a definition

of a security policy. Option C is a formal evaluation of the security of a system. Option D is the definition of virtualization.

13. D. The Bell–LaPadula and Biba models are built on the state machine model. Take-Grant and Clark–Wilson are not directly based or built on the state machine model.
14. A. Only the Bell–LaPadula model addresses data confidentiality. The Biba and Clark–Wilson models address data integrity. The Brewer and Nash model prevents conflicts of interest.
15. C. The no read-up property, also called the simple security property, prohibits subjects from reading a higher security level object. The other options are incorrect. Option A, the (star) security property of Bell–LaPadula, is no write-down. Option B, no write-up, is the (star) property of Biba. Option D, no read-down, is the simple property of Biba.
16. B. The simple property of Biba is no read-down, but the implied allowed opposite is read-up. The other options are incorrect. Option A, write-down, is the implied opposite allow of the (star) property of Biba, which is no write-up. Option C, no write-up, is the (star) property of Biba. Option D, no read-down, is the simple property of Biba.
17. D. Security targets (STs) specify the vendor's security claims that are built into a target of evaluation (TOE). STs are considered the implemented security measures or the “I will provide” from the vendor. The other options are incorrect. Option A, protection profiles (PPs), specify the security requirements and protections for a product that is to be evaluated (the TOE), which are considered the security desires or the “I want” from a customer. Option B, evaluation assurance levels (EALs), are the various levels of testing and confirmation of systems' security capabilities, and the number of the level indicates what kind of testing and confirmation has been performed. Option C, an authorizing official (AO), is the entity with the authority to issue an authorization to operate (ATO).
18. A, C, E. The four types of ATOs are authorization to operate (not listed as an option), common control authorization,

authorization to use, and denial of authorization. The other options are incorrect.

19. B. Memory protection is a core security component that must be designed and implemented into an operating system. It must be enforced regardless of the programs executing in the system. Otherwise, instability, violation of integrity, denial of service, and disclosure are likely results. The other options are incorrect. Option A, the use of virtualization, would not cause all of those security issues. Option C, the Clark–Wilson model based on the access control triplet is about protecting integrity through a restricted interface, and thus is not the cause of the issues of this scenario. Option D, the use of encryption, is a protection, not a cause of these security issues.

20. A. A constrained or restricted interface is implemented within an application to restrict what users can do or see based on their privileges. The purpose of a constrained interface is to limit or restrict the actions of both authorized and unauthorized users. The other options are incorrect. Option B describes authentication. Option C describes auditing and accounting. Option D describes virtual memory.

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

1. A, C, D, F. The statements in options A, C, D, and F are all valid elements or considerations of shared responsibility. The other options are incorrect. Always consider the threat to both tangible and intangible assets as a tenet of risk management and BIA. Multiple layers of security are required to protect against adversary attempts to gain access to internal sensitive resources and is a general principle of security known as defense in depth.
2. C. Multitasking is processing more than one task at the same time. In most cases, multitasking is simulated by the OS (using multiprogramming or pseudo-simultaneous execution) even when not supported by the processor. Multicore (not listed as an option) is also able to perform simultaneous execution but does so with multiple execution cores on one or more CPUs. Multistate is a type of system that can operate at various security levels (or classifications, risk levels, etc.). Multithreading permits multiple concurrent tasks (i.e., threads) to be performed within a single process. In a multiprocessing environment, a multiprocessor computing system (that is, one with more than one CPU) harnesses the power of more than one processor to complete the execution of a multithreaded application.
3. C. JavaScript remains the one mobile code technology that may affect the security of modern browsers and their host OSs. Java is deprecated for general internet use, and browsers do not have native support for Java. A Java add-on is still available to install, but it is not preinstalled, and general security guidance recommends avoiding it on any internet-facing browser. Flash is deprecated; no modern browser supports it natively. Adobe has abandoned it, and most browsers actively block the add-on. ActiveX is also deprecated, and though it was always only a Microsoft Windows technology, it was only supported by Internet Explorer, not Edge (either in its original form or the more recent Chromium-based version). Although Internet Explorer was present on the original Windows 10, this scenario

stated that all other browsers were deactivated or blocked. Thus, this scenario is limited to the latest Edge browser. This question assumes you understand the latest version of Windows is Windows 11 and the latest version of Microsoft's browser is Edge (as of Q1 2024).

4. A. In many grid computing implementations, grid members can access the contents of the distributed work segments or divisions. This grid computing over the Internet is not usually the best platform for sensitive operations. Grid computing is able to handle and compensate for latency of communications, duplicate work, and capacity fluctuation.
5. B. Option B references a VDI or VMI instance that serves as a virtual endpoint for accessing cloud assets and services, but this concept is not specifically relevant to or a requirement of this scenario. The remaining items are relevant to the selection process in this scenario. These are all compute security–related concepts. Option A, security groups, are collections of entities, typically users, but can also be applications and devices, which can be granted or denied access to perform specific tasks or access certain resources or assets. This supports the requirement of controlling which applications can access which assets. Option C, dynamic resource allocation (aka elasticity), is the ability of a cloud process to use or consume more resources (such as compute, memory, storage, or networking) when needed. This supports the requirement of processing significant amounts of data in short periods of time. Option D is a management or security mechanism, which is able to monitor and differentiate between numerous instances of the same VM, service, app, or resource. This supports the requirement of prohibiting VM sprawl or repetition of operations.
6. D. A large utility company is very likely to be using supervisory control and data acquisition (SCADA) to manage and operate their equipment; therefore, that is the system that the APT group would have compromised. A multifunction printer (MFP) is not likely to be the attack point that granted the APT group access to the utility distribution nodes. A real-time OS (RTOS) may have been present on some of the utility company's

systems, but that is not the obvious target for an attack to take over control of an entire utility service. There may be system on chip (SoC) equipment present at the utility, but that would still be controlled and accessed through the SCADA system at a utility company.

7. C. Secondary memory is a term used to describe magnetic, optical, or flash media (i.e., typical storage devices like HDD, SSD, CD, DVD, and thumb drives). These devices will retain their contents after being removed from the computer and may later be read by another user. Static RAM and dynamic RAM are types of real memory and thus are all the same concept in relation to being volatile—meaning they lose any data they were holding when power is lost or cycled. Static RAM is faster and more costly, and dynamic RAM requires regular refreshing of the stored contents. Take notice in this question that three of the options were effectively synonyms (at least from the perspective of volatile versus nonvolatile storage). If you notice synonyms among answer options, realize that none of the synonyms can be a correct answer for single-answer multiple-choice questions.

8. C. The primary security concern of a distributed computing environment (DCE) is the interconnectedness of the components. This configuration could allow for error or malware propagation as well. If an adversary compromises one component, it may grant them the ability to compromise other components in the collective through pivoting and lateral movement. The other options are incorrect. Unauthorized user access, identity spoofing, and poor authentication are potential weaknesses of most systems; they are not unique to DCE solutions. However, these issues can be directly addressed through proper design, coding, and testing. However, the interconnectedness of components is a native characteristic of DCE that cannot be removed without discarding the DCE design concept itself.

9. C. The best means to reduce IoT risk from these options is to keep devices current on updates. Using public IP addresses will expose the IoT devices to attack from the internet. Powering off devices is not a useful defense—the benefit of IoT is that they are

always running and ready to be used or take action when triggered or scheduled. Blocking access to the Internet will prevent the IoT devices from obtaining updates themselves, may prevent them from being controlled through a mobile device app, and will prevent communication with any associated cloud service.

10. D. Microservices are an emerging feature of web-based solutions and are derivative of service-oriented architecture (SOA). A microservice is simply one element, feature, capability, business logic, or function of a web application that can be called upon or used by other web applications. It is the conversion or transformation of a capability of one web application into a microservice that can be called upon by numerous other web applications. The relationship to an application programming interface (API) is that each microservice must have a clearly defined (and secured!) API to allow for I/O between multi-microservices as well as to and from other applications. The other options are incorrect since they are not derivatives of SOA. Cyber-physical systems are devices that offer a computational means to control something in the physical world. Fog computing relies on sensors, IoT devices, or even edge computing devices to collect data and then transfer it back to a central location for processing. Distributed control systems (DCSs) are typically found in industrial process plants where the need to gather data and implement control over a large-scale environment from a single location is essential.

11. B. This scenario describes the systems as being nonpersistent. A nonpersistent system or static system is a computer system that does not allow, support, or retain changes. Thus, between uses and/or reboots, the operating environment and installed software are exactly the same. Changes may be blocked or simply discarded after each system use. A nonpersistent system is able to maintain its configuration and security in spite of user attempts to implement change. This scenario is not describing a cloud solution, although a virtual desktop infrastructure (VDI) could be implemented on-premises or in the cloud. This scenario is not describing thin clients, since the existing “standard” PC endpoints are still in use but a VDI is being used

instead of the local system capabilities. A VDI deployment simulates a thin client. This scenario is not describing fog computing. Fog computing relies on sensors, IoT devices, or even edge computing devices to collect data and then transfer it back to a central location for processing.

12. B. The issue in this situation is VM sprawl. Sprawl occurs when organizations fail to plan their IT/IS needs and just deploy new systems, software, and VMs whenever their production needs demand it. This often results in obtaining underpowered equipment that is then overtaxed by inefficient implementations of software and VMs. This situation is not specifically related to end-of-service-life (EOSL) systems, but EOSL systems would exacerbate the sprawl issue. This situation is not related to poor cryptography, nor is there any evidence of VM escaping issues.

13. C. Containerization is based on the concept of eliminating the duplication of OS elements in a virtual machine. Instead, each application is placed into a container that includes only the actual resources needed to support the enclosed application, and the common or shared OS elements are then part of the hypervisor. The system as a whole could be redeployed using a containerization solution, and each of the applications previously present in the original seven VMs could be placed into containers, as well as the six new applications. This should result in all 13 applications being able to operate reasonably well without the need for new hardware. Data sovereignty is the concept that, once information has been converted into a binary form and stored as digital files, it is subject to the laws of the country within which the storage device resides. Infrastructure as code (IaC) is a change in how hardware management is perceived and handled. Instead of seeing hardware configuration as a manual, direct hands-on, one-on-one administration hassle, it is viewed as just another collection of elements to be managed in the same way that software and code are managed under DevSecOps (security, development, and operations). Process isolation requires that the OS provide separate memory spaces for each process's instructions and data and that the OS enforce those boundaries, preventing one

process from reading or writing data that belongs to another process.

14. B. In industrial control systems (ICSs), ensuring the availability of real-time control signals is a primary concern. Confidentiality, integrity, and nonrepudiation are important security concerns, but the immediate and continuous availability of control signals is critical for the proper functioning of industrial processes.

15. C. Because an embedded system is often in control of a mechanism in the physical world, a security breach could cause harm to people and property (aka cyber-physical). This typically is not true of a standard PC. Power loss, internet access, and software flaws are security risks of both embedded systems and standard PCs.

16. A. Arduino is a microcontroller that can be used to perform automated tasks. MPP (massive parallel processing) systems are too expensive and not a reasonable option for this scenario. A real-time operating system (RTOS) is designed to process or handle data as it arrives on the system with minimal latency or delay. RTOS is a software OS that is usually stored and executed from ROM and thus may be part of an embedded solution or hosted on a microcontroller. An RTOS is designed for mission-critical operations where delay must be eliminated or minimized for safety. Thus, RTOS is not the best option for this scenario since it is about managing a garden, which does not need real-time mission-critical operations. A field-programmable gate array (FPGA) is a flexible computing device intended to be programmed by the end user or customer. FPGAs are often used as embedded devices in a wide range of products, including industrial control systems (ICSs). FPGAs can be challenging to program and are often more expensive than other more limited solutions. Thus, FPGA is not the best fit for this scenario.

17. D. This scenario is describing a product that requires a real-time operating system (RTOS) solution, since it mentions the need to minimize latency and delay, storing code in ROM, and optimizing for mission-critical operations. A containerized application is not a good fit for this situation because it may not be able to operate in near real time due to the virtualization

infrastructure, and containerized apps are typically stored as files on the contain host rather than a ROM chip. An Arduino is a type of microcontroller, but not typically robust enough to be considered a near-real-time mechanism; it stores code on a flash chip, has a limited C++ based instruction set, and is not suited for mission-critical operations. A distributed control system (DCS) can be used to manage small-scale industrial processes, but it is not designed as a near-real-time solution. DCSs are not stored in ROM, but they may be used to manage mission-critical operations.

18. A. This scenario is an example of edge computing. In edge computing, the intelligence and processing is contained within each device. Thus, rather than having to send data off to a master processing entity, each device can process its own data locally. The architecture of edge computing performs computations closer to the data source, which is at or near the edge of the network. Fog computing relies on sensors, IoT devices, or even edge computing devices to collect data and then transfer it back to a central location for processing. A thin client is a computer with low to modest capability or a virtual interface that is used to remotely access and control a mainframe, virtual machine, or virtual desktop infrastructure (VDI). Infrastructure as code (IaC) is a change in how hardware management is perceived and handled. Instead of seeing hardware configuration as a manual, direct hands-on, one-on-one administration hassle, it is viewed as just another collection of elements to be managed in the same way that software and code are managed under DevOps.
19. B. The risk of a lost or stolen laptop is the data loss, not the loss of the system itself, but the value of the data on the system, whether business related or personal. Thus, keeping minimal sensitive data on the system is the only way to reduce the risk. Hard drive encryption, cable locks, and strong passwords, although good ideas, are preventive tools, not means of reducing risk. They don't keep intentional and malicious data compromise from occurring; instead, they encourage honest people to stay honest. Hard drive encryption can be bypassed using the cold boot attack or by taking advantage of an

encryption service flaw or configuration mistake. Cable locks can be cut or ripped out of the chassis. Strong passwords do not prevent the theft of a device, and password cracking and/or credential stuffing may be able to overcome the protection. If not, the drive could be extracted and connected to another system to access files directly, even with the native OS running.

20. D. The best option in this scenario is corporate-owned. A corporate-owned mobile strategy (COMS) or corporate-owned, business-only (COBO) is when the company purchases mobile devices that can support compliance with the security policy. These devices are to be used exclusively for company purposes, and users should not perform any personal tasks on them. This option often requires workers to carry a second device for personal use. Corporate-owned clearly assigns responsibility for device oversight to the organization. The other three options still allow for comingling of data and have unclear or vague security responsibility assignments as a concept or policy basis. BYOD is a policy that allows employees to bring their own personal mobile devices to work and use those devices to connect to business resources and/or the Internet through the company network. The concept of corporate-owned, personally enabled (COPE) means the organization purchases devices and provides them to employees. Each user is then able to customize the device and use it for both work activities and personal activities. The concept of choose your own device (CYOD) provides users with a list of approved devices from which to select the device to implement.

Chapter 10: Physical Security Requirements

1. C. Natural training and enrichment is not a core strategy of first generation CPTED. Crime Prevention Through Environmental Design (CPTED) has four main strategies: access control, natural surveillance, image and milieu, and territorial control. Access control is the subtle guidance of those entering and leaving a building through the placement of entranceways, fences, bollards, and lights. Natural surveillance is any means to make criminals feel uneasy through the increasing opportunities for them to be observed. Territorial control is the attempt to make the area feel like an inclusive, caring community.
2. B. Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations and all the necessary supporting elements when evaluating the security of a facility or designing a new facility. Log file audit can help detect violations to hold users accountable, but it is not a security facility design element. Risk analysis is often involved in facility design, but it is the evaluation of threats against assets regarding the rate of occurrence and levels of consequence. Taking inventory is an important part of facility and equipment management but is not an element in overall facility design.
3. A, C, F. The true statements are option A, cameras should be positioned to watch exit and entry points; option C, cameras should be positioned to have clear sight lines of all exterior walls, entrance and exit points, and interior hallways; and option F, some camera systems include a system on a chip (SoC) or embedded components and may be able to perform various specialty functions, such as time-lapse recording, tracking, facial recognition, object detection, or infrared or color-filtered recording. The remaining answer options are incorrect. The corrected statements for those options are: option B: cameras should be used to monitor activities around valuable assets and resources as well as to provide additional protection in public areas such as parking structures and walkways; option D:

security cameras can be overt and obvious to provide a deterrent benefit, or hidden and concealed to primarily provide a detection benefit; option E: some cameras are fixed, whereas others support remote control of automated pan, tilt, and zoom (PTZ); and option G: simple motion recognition or motion-triggered cameras may be fooled by animals, birds, insects, weather, or foliage.

4. D. Equal access to all locations within a facility is not a security-focused design element. Each area containing assets or resources of different importance, value, and confidentiality should have a corresponding level of security restriction placed on it. A secure facility should have a separation between work and visitor areas and should restrict access to areas with higher value or importance, and confidential assets should be located in the heart or center of a facility.
5. A. A computer room does not need to be optimized for human workers to be efficient and secure. A server room would be more secure with a nonwater fire suppressant system (it would protect against damage caused by water suppressant). A server room should have humidity maintained between 20 and 80 percent relative humidity and temperature maintained between 59 and 89.6 degrees Fahrenheit.
6. C. Hashing is not a typical security measure implemented in relation to a media storage facility containing reusable, removable media. Hashing is used when it is necessary to verify the integrity of a dataset, whereas data on reusable removable media should be removed and not retained. Usually, the security features for a media storage facility include using a media librarian or custodian, using a check-in/checkout process, and using sanitization tools on returned media.
7. B. The humidity in a computer room should ideally be from 20 to 80 percent. Humidity above 80 percent can result in condensation, which causes corrosion. Humidity below 20 percent can result in increased static electricity buildup. However, this does require managing temperature properly as well. The other number ranges are not the relative humidity ranges recommended for a data center.

8. B, C, E, F, H. The primary elements of a cable plant management policy should include a mapping of the entrance facility (i.e., demarcation point), equipment room, backbone distribution system, telecommunications room, and horizontal distribution system. The other items are not elements of a cable plant. Thus, person traps, fire escapes, UPSs, and the loading dock are not needed elements on a cable map.
9. C. A preaction system is the best type of water-based fire suppression system for a computer facility because it provides the opportunity to prevent the release of water in the event of a false alarm or false initial trigger. The other options of wet pipe, dry pipe, and deluge system use only a single trigger mechanism without the ability to prevent accidental water release.
10. B. Human error is the most common cause of a false positive for a water-based system. If you turn off the water source after a fire and forget to turn it back on, you'll be in trouble in the future. Also, pulling an alarm when there is no fire will trigger damaging water release throughout the office. Water shortage would be a problem, but it is not a cause for a false positive event. Ionization detectors are highly reliable, so they are usually not the cause of a false positive event. Detectors can be placed in drop ceilings to monitor that air space; this would only be a problem if another detector was not placed in the room's main area. If there are only detectors in the drop ceiling, then that could result in a false negative event.
11. D. The cause of the hardware failures is implied by the lack of organization of the equipment, which is heat buildup. This could be addressed by better managing temperature and airflow, which would involve implementing hot and cold aisles in the data center. A data center should have few, if any, actual visitors (such as outsiders), but anyone entering and leaving a data center should be tracked and recorded in a log. However, whether or not a visitor log is present has little to do with system failure due to poor heat management. Industrial camouflage is not relevant here since it is about hiding the purpose of a facility from outside observers. A gas-based fire suppression system is more appropriate for a data center than a water-based system,

but neither would cause heat problems due to poor system organization.

12. B, C, D. Benefits of gas-based fire suppression include causing the least damage to computer systems and extinguishing the fire quickly by removing oxygen. Also, gas-based fire suppression may be more effective and faster than a water-based system. A gas-based fire suppression system can only be used where human presence is at a minimum, since it removes oxygen from the air.

13. B. The correct order of the six common physical security control mechanisms is Deter, Deny, Detect, Delay, Determine, Decide. The other options are incorrect.

14. C. Mean time to failure (MTTF) is the expected typical functional lifetime of the device given a specific operating environment. Mean time to repair (MTTR) is the average length of time required to perform a repair on the device. Mean time between failures (MTBF) is an estimation of the time between the first and any subsequent failures. A service-level agreement (SLA) clearly defines the response time a vendor will provide in the event of an equipment failure emergency.

15. C. Human safety is the most important goal of all security solutions. The top priority of security should always be the protection of the lives and safety of personnel. The protection of CIA (confidentiality, integrity, and availability) of company data and other assets is the second priority after human life and safety.

16. C. A person trap is a double set of doors often protected by a guard and used to contain a subject until their identity and authentication is verified. A gate is a doorway used to traverse through a fence line. A turnstile is an ingress or egress point that allows travel only in one direction and by one person at a time. A proximity detector determines whether a proximity device is nearby and whether the bearer is authorized to access the area being protected.

17. D. Lighting is often claimed to be the most commonly deployed physical security mechanism. However, lighting is only a

deterrent and not a strong deterrent. It should not be used as the primary or sole protection mechanism except in areas with a low threat level. Your entire site, inside and out, should be well lit. This provides for easy identification of personnel and makes it easier to notice intrusions. Security guards are not as common as lighting, but they are more flexible in terms of security benefits. Fences are not as common as lighting, but they serve as a preventive control. CCTV is not as common as lighting but serves as a detection control.

18. A. Security guards are usually unaware of the scope of the operations within a facility and are therefore not thoroughly equipped to know how to respond to every situation. Though this is considered a disadvantage, the lack of knowledge of the scope of the operations within a facility can also be considered an advantage because this supports confidentiality of those operations and thus helps reduce the possibility that a security guard will be involved in the disclosure of confidential information. Thus, even though this answer option is ambiguous, it is still better than the three other options. The other three options are disadvantages of security guards. Not all environments and facilities support security guards. This may be because of actual human incompatibility or the layout, design, location, and construction of the facility. Not all security guards are themselves reliable. Prescreening, bonding, and training do not guarantee that you won't end up with an ineffective or unreliable security guard.

19. C. Key locks are the most common and inexpensive form of physical access control device for both interior and exterior use. Lighting, security guards, and fences are all much more costly. Fences are also mostly used outdoors.

20. D. A capacitance motion detector senses changes in the electrical or magnetic field surrounding a monitored object. A wave pattern motion detector transmits a consistent low ultrasonic or high microwave frequency signal into a monitored area and monitors for significant or meaningful changes or disturbances in the reflected pattern. A photoelectric motion detector senses changes in visible light levels for the monitored

area. Photoelectric motion detectors are usually deployed in internal rooms that have no windows and are kept dark. An infrared PIR (passive infrared) or heat-based motion detector monitors for significant or meaningful changes in the heat levels and patterns in a monitored area.

Chapter 11: Secure Network Architecture and Components

1. A. The SYN flagged packet is first sent from the initiating host to the destination host; thus, it is the first step or phase in the TCP three-way handshake sequence used to establish a TCP session. The destination host then responds with a SYN/ACK flagged packet; this is the second step or phase of the TCP three-way handshake sequence. The initiating host sends an ACK flagged packet, and the connection is then established (the final or third step or phase). The FIN flag is used to gracefully shut down an established session.
2. D. UDP is a simplex protocol at the Transport Layer (Layer 4 of the OSI model). Bits are associated with the Physical Layer (Layer 1). Logical addressing is associated with the Network Layer (Layer 3). Data reformatting is associated with the Presentation Layer (Layer 6).
3. A, B, D. The means by which IPv6 and IPv4 can coexist on the same network is to use one or more of three primary options: dual stack, tunneling, or NAT-PT. Dual stack is to have most systems operate both IPv4 and IPv6 and use the appropriate protocol for each conversation. Tunneling allows most systems to operate a single stack of either IPv4 or IPv6 and use an encapsulation tunnel to access systems of the other protocol. Network Address Translation-Protocol Translation (NAT-PT) (RFC-2766) can be used to convert between IPv4 and IPv6 network segments similar to how NAT converts between internal and external addresses. IPSec is a standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6, but it does not enable the use of both IPv4 and IPv6 on the same system (although it doesn't prevent it either). IP sideloading is not a real concept.
4. A, B, E. TLS allows for use of TCP port 443; prevents tampering, spoofing, and eavesdropping; and can be used as a VPN solution. The other options are incorrect. TLS supports both

one-way and two-way authentication. TLS and SSL are not interoperable or backward compatible.

5. B. Encapsulation is both a benefit and a potentially harmful implication of multilayer protocols. Encapsulation allows for encryption, flexibility, and resiliency, while also enabling covert channels, filter bypass, and overstepping network segmentation boundaries. Throughput is the capability of moving data across or through a network; this is not an implication of multilayer protocols. Hash integrity checking is a common benefit of multilayer protocols because most layers include a hash function in their header or footer. Logical addressing is a benefit of multilayer protocols; this avoids the restriction of using only physical addressing.
6. C. In this scenario, the only viable option to provide performance, availability, and security for the VoIP service is to implement a new, separate network for the VoIP system that is independent of the existing data network. The current data network is already at capacity, so creating a new VLAN will not provide sufficient insurance that the VoIP service will be highly available. Replacing switches with routers is usually not a valid strategy for increasing network capacity, and 1,000 Mbps is the same as 1 Gbps. Flood guards are useful against DoS and some transmission errors (such as Ethernet floods or broadcast storms), but they do not add more capacity to a network or provide reliable uptime for a VoIP service.
7. B, C, E. Micro-segmentation can be implemented using internal segmentation firewalls (ISFWs), transactions between zones are filtered, and it can be implemented with virtual systems and virtual networks. Affinity or preference is the assignment of the cores of a CPU to perform different tasks. Micro-segmentation is not related to edge and fog computing management.
8. A. The device in this scenario would benefit from the use of Zigbee. Zigbee is an IoT equipment communications concept that is based on Bluetooth. Zigbee has low power consumption and a low throughput rate, and it requires close proximity of devices. Zigbee communications are encrypted using a 128-bit symmetric algorithm. Bluetooth is not a good option since it is

usually plaintext. Bluetooth Low Energy (BLE) might be a viable option if custom encryption was added. Geostationary orbit (GEO) satellite internet service would offer slower throughput with higher latency compared to terrestrial options, and while it may offer encryption, it is not an appropriate option for this scenario. 5G is the latest mobile service technology that is available for use on mobile phones, tablets, and other equipment. Though many IoT devices may support and use 5G, it is mostly used to provide direct access to the Internet rather than as a link to a local short-distance device, such as a PC or IoT hub.

9. A, B, D. Cellular services, such as 4G and 5G, raise numerous security and operational concerns. Although cellular service is encrypted from device to tower, there is a risk of being fooled by a false or rogue tower. A rogue tower could offer only plaintext connections, but even if it supported encrypted transactions, the encryption only applies to the radio transmissions between the device and the tower. Once the communication is on the tower, it will be decrypted, allowing for eavesdropping and content manipulation. Even without a rogue tower, eavesdropping can occur across the cellular carrier's interior network as well as across the Internet, unless a VPN link is established between the remote mobile device and the network of the organization James works for. Being able to establish a connection can be unreliable depending on exactly where James's travel takes him. 4G and 5G coverage is not 100 percent available everywhere. Each 5G tower covers less area than a 4G tower. If James is able to establish a connection, 4G and 5G speeds should be sufficient for most remote technician activities, since 4G supports 100 Mbps for mobile devices, and 5G supports up to 10 Gbps. If connectivity is established, there should be no issues with cloud interaction or duplex conversations.

10. B. A content distribution network (CDN), or content delivery network, is a collection of resource service hosts deployed in numerous data centers across the world to provide low latency, high performance, and high availability of the hosted content. VPNs are used to transport communications over an intermediary medium through the means of encapsulation (i.e.,

tunneling), authentication, and encryption. Software-defined networking (SDN) aims at separating the infrastructure layer from the control layer on networking hardware to reduce management complexity. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) (Counter-Mode/CBC-MAC Protocol) is the combination of two block cipher modes to enable streaming by a block algorithm.

11. D. The true statement is: ARP poisoning can use unsolicited or gratuitous replies—specifically, ARP replies for which the local device did not transmit an ARP broadcast request. Many systems accept all ARP replies regardless of who requested them. The other statements are false. The correct versions of those statements would be: (A) MAC flooding is used to overload the memory of a switch, specifically the CAM table stored in switch memory when bogus information will cause the switch to function only in flooding mode. (B) MAC spoofing is used to falsify the physical address of a system to impersonate that of another authorized device. ARP poisoning associates an IP address with the wrong MAC address. (C) MAC spoofing relies on plaintext Ethernet headers to initially gather valid MAC addresses of legitimate network devices. ICMP crosses routers because it is carried as the payload of an IP packet.

12. D. The most likely cause of the inability to recover files from the SAN in this scenario is deduplication. Deduplication replaces multiple copies of a file with a pointer to one copy. If the one remaining file is damaged, then all of the linked copies are damaged or inaccessible as well. File encryption could be an issue, but the scenario mentions that groups of people work on projects, and, typically, file encryption is employed by individuals, not by groups. Whole-drive encryption would be more appropriate for group-accessed files as well as for an SAN in general. This issue is not related to what SAN technology is used, such as Fibre Channel. This problem might be solvable by restoring files from a backup, whether real-time or not, but the loss of files is not caused by performing backups.

13. D. In this scenario, the malware is performing a MAC flooding attack, which causes the switch to get stuck in flooding mode.

This has taken advantage of the condition that the switch had weak configuration settings. The switch should have MAC limiting enabled to prevent MAC flooding attacks from being successful. Although Jim was initially fooled by a social engineering email, the question asked about the malware's activity. A MAC flooding attack is limited by network segmentation to the local switch, but the malware took advantage of weak or poor configuration on the switch and was still successful. MAC flooding is blocked by routers from crossing between switched network segments. The malware did not use ARP queries in its attack. ARP queries can be abused in an ARP poisoning attack, but that was not described in this scenario.

14. B. A switch is an intelligent hub. It is considered to be intelligent because it knows the addresses of the systems connected on each outbound port. Repeaters are used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol. A bridge is used to connect two networks together—even networks of different topologies, cabling types, and speeds—to connect network segments that use the same protocol. Routers are used to control traffic flow on networks and are often used to connect similar networks and control traffic flow between the two. Routers manage traffic based on logical IP addressing.

15. B. A screened subnet is a type of security zone that can be positioned so that it operates as a buffer network between the secured private network and the Internet and can host publicly accessible services. A honeypot is a false network used to trap intruders; it isn't used to host public services. An extranet is for limited outside partner access, not public. An intranet is the private secured network.

16. B. A Faraday cage is an enclosure that blocks or absorbs electromagnetic fields or signals. Faraday cage containers, computer cases, rack-mount systems, rooms, or even building materials are used to create a blockage against the transmission of data, information, metadata, or other emanations from computers and other electronics. Devices inside a Faraday cage

can use EM fields for communications, such as wireless or Bluetooth, but devices outside of the cage will not be able to eavesdrop on the signals of the systems within the cage. Air gaps do not contain or restrict wireless communications—in fact, for an air gap to be effective, wireless cannot even be available. Biometric authentication has nothing to do with controlling radio signals. Screen filters reduce shoulder surfing but do not address radio signals.

17. B, E, F. Network access control (NAC) involves controlling access to an environment through strict adherence to and implementation of security policy. The goals of NAC are to detect/block rogue devices, prevent or reduce zero-day attacks, confirm compliance with updates and security settings, enforce security policy throughout the network, and use identities to perform access control. NAC does not address social engineering, mapping IP addresses, or distributing IP addresses —those are handled by training, NAT, and DHCP, respectively.

18. A. Endpoint detection and response (EDR) is a security mechanism that is an evolution of traditional antimalware products. EDR seeks to detect, record, evaluate, and respond to suspicious activities and events, which may be caused by problematic software or by valid and invalid users. It is a natural extension of continuous monitoring, focusing on both the endpoint device itself and network communications reaching the local interface. Some EDR solutions employ an on-device analysis engine whereas others report events back to a central analysis server or to a cloud solution. The goal of EDR is to detect abuses that are potentially more advanced than what can be detected by traditional antivirus or HIDSs, while optimizing the response time of incident response, discarding false positives, implementing blocking for advanced threats, and protecting against multiple threats occurring simultaneously and via various threat vectors. A next-generation firewall (NGFW) is a unified threat management (UTM) device that is based on a traditional firewall with numerous other integrated network and security services and is thus not the security solution needed in this scenario. A web application firewall (WAF) is an appliance, server add-on, virtual service, or system

filter that defines a strict set of communication rules for a website and is not the security solution needed in this scenario. Cross-site request forgery (XSRF) is an attack against web-based services, not a malware defense.

19. A. An application-level firewall is able to make access control decisions based on the content of communications as well as the parameters of the associated protocol and software. Stateful inspection firewalls make access control decisions based on the content and context of communications, but are not typically limited to a single application-layer protocol. Circuit-level firewalls are able to make permit and deny decisions in regard to circuit establishment either based on simple rules for IP and port, using captive portals, requiring port authentication via 802.1X, or more complex elements such as context- or attribute-based access control. Static packet-filtering firewalls filter traffic by examining data from a message header. Usually, the rules are concerned with source and destination IP address (Layer 3) and port numbers (Layer 4).

20. A, C, D. Most appliance (i.e., hardware) firewalls offer extensive logging, auditing, and monitoring capabilities as well as alarms/alerts and even basic IDS functions. It is also true that firewalls are unable to prevent internal attacks that do not cross the firewall. Firewalls are unable to block new phishing scams. Firewalls could block a phishing scam's URL if it was already on a block list, but a new scam likely uses a new URL that is not yet known to be malicious.

Chapter 12: Secure Communications and Network Attacks

1. B. When transparency is a characteristic of a service, security control, or access mechanism, it is unseen by users. Invisibility is not the proper term for a security control that goes unnoticed by valid users. Invisibility is sometimes used to describe a feature of a rootkit, which attempts to hide itself and other files or processes. Diversion is a feature of a honeypot but not of a typical security control. Hiding in plain sight is not a security concept; it is a mistake on the part of the observer not to notice something that they should notice. This is not the same concept as camouflage, which is when an object or subject attempts to blend into the surroundings.
2. A, C, D, E, G, I, J, K. More than 40 EAP methods have been defined, including LEAP, PEAP, EAP-SIM, EAP-FAST, EAP-MD5, EAP-POTP, EAP-TLS, and EAP-TTLS. The other options are not valid EAP methods.
3. B. Changing default passwords on PBX systems provides the most effective increase in security. PBX systems typically do not support encryption, although some VoIP PBX systems may support encryption in specific conditions. PBX transmission logs may provide a record of fraud and abuse, but they are not a preventive measure to stop it from happening. Taping and archiving all conversations is also a detection measure rather than a preventive one against fraud and abuse.
4. C. Malicious attackers known as phreakers abuse phone systems in much the same way that attackers abuse computer networks. In this scenario, they were most likely focused on the PBX. Private branch exchange (PBX) is a telephone switching or exchange system deployed in private organizations in order to enable multistation use of a small number of external PSTN lines. Phreakers generally do not focus on accounting (that would be an invoice scam), NAT (that would be a network

intrusion attack), or Wi-Fi (another type of network intrusion attack).

5. A, B, D. It is important to verify that multimedia collaboration connections are encrypted, that robust multifactor authentication is in use, and that tracking and logging of events and activities is available for the hosting organization to review. Customization of avatars and filters is not a security concern.
6. D. The issue in this scenario is that a private IP address from RFC 1918 is assigned to the web server. RFC 1918 addresses are not internet routable or accessible because they are reserved for private or internal use only. So, even with the domain name linked to the address, any attempt to access it from an internet location will fail. Local access via jumpbox or LAN system likely uses an address in the same private IP address range and has no issues locally. The issue of the scenario (i.e., being unable to access a website using its FQDN) could be resolved by either using a public IP address or implementing static NAT on the screened subnet's boundary firewall. The jumpbox would not prevent access to the website regardless of whether it was rebooted, in active use, or turned off. That would only affect Michael's use of it from his desktop workstation. Split-DNS does support internet-based domain name resolution; it separates internal-only domain information from external domain information. A web browser should be compatible with the coding of most websites. Since there was no mention of custom coding and the site was intended for public use, it is probably using standard web technologies. Also, since Michael's workstation and several worker desktops could access the website, the problem is probably not related to the browser.
7. A. Password Authentication Protocol (PAP) is a standardized authentication protocol for PPP. PAP transmits usernames and passwords in the clear. It offers no form of encryption. It provides a means to transport the logon credentials from the client to the authentication server. CHAP protects the password by never sending it across the network; it is used in computing a response along with a random challenge number issued by the server. EAP offers some means of authentication that protects

and/or encrypts credentials, but not all of the options do. RADIUS supports a range of options to protect and encrypt logon credentials.

8. A, C, D, F, G, H, and J. Network quality of service (QoS) depends on numerous factors, including bandwidth, latency, jitter, packet loss, interference, throughput, and signal-to-noise ratio. System uptime, application layer protocol, and OS versions are unlikely to be relevant related to network QoS investigations.
9. A, C, D. The addresses in RFC 1918 are 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255, and 192.168.0.0–192.168.255.255. Therefore, 10.0.0.18, 172.31.8.204, and 192.168.6.43 are private IPv4 addresses. The 169.254.x.x subnet is in the APIPA range, which is not part of RFC 1918.
10. D. An intermediary network connection is required for a VPN link to be established. A VPN can be established between devices over the Internet, between devices over a LAN, or between a system on the Internet and a LAN.
11. B. A switch is a networking device that can be used to create digital virtual network segments (i.e., VLANs) that can be altered as needed by adjusting the settings internal to the device. A router connects disparate networks (i.e., subnets) rather than creating network segments. Subnets are created by IP address and subnet mask assignment. Proxy and firewall devices do not create digital virtual network segments, but they may be positioned between network segments to control and manage traffic.
12. B. VLANs do not impose encryption on data or traffic. Encrypted traffic can occur within a VLAN, but encryption is not imposed by the VLAN. VLANs do provide traffic isolation, traffic management and control, and a reduced vulnerability to sniffers.
13. B, C, D. Port security can refer to several concepts, including network access control (NAC), Transport Layer ports, and RJ-45 jack ports. NAC requires authentication before devices can communicate on the network. Transport-layer port security involves using firewalls to grant or deny communications to TCP

and UDP ports. RJ-45 jacks should be managed so that unused ports are disabled and that when a cable is disconnected, the port is disabled. This approach prevents the connection of unauthorized devices. Shipping container storage relates to shipping ports, which is a type of port that is not specifically related to IT or typically managed by a CISO.

14. B. Quality of service (QoS) is the oversight and management of the efficiency and performance of network communications. Items to measure include throughput rate, bit rate, packet loss, latency, jitter, transmission delay, and availability. A virtual private network (VPN) is a communication channel between two entities across an intermediary untrusted network. Software-defined networking (SDN) aims at separating the infrastructure layer from the control layer on networking hardware in order to reduce management complexity. Sniffing captures network packers for analysis. QoS uses sniffing, but sniffing itself is not QoS.

15. D. When IPSec is used in tunnel mode, entire packets, rather than just the payload, are encrypted. Transport mode only encrypts the original payload, not the original header. Encapsulating Security Payload (ESP) is the encrypter of IPSec, not the mode of VPN connection. Authentication Header (AH) is the primary authentication mechanism of IPSec.

16. A. Authentication Header (AH) provides assurances of message integrity and identity verification (i.e., authentication). Encapsulating Security Payload (ESP) provides confidentiality and integrity of payload contents. ESP also provides encryption, offers limited authentication, and prevents replay attacks. IP Payload Compression (IPComp) is a compression tool used by IPSec to compress data prior to ESP encrypting it in order to attempt to keep up with wire speed transmission. Internet Key Exchange (IKE) is the mechanism of IPSec that manages cryptography keys and is composed of three elements: OAKLEY, SKEME, and ISAKMP.

17. B. Data remanent destruction is a security concern related to storage technologies more so than an email solution. Essential email concepts, which local systems can enforce and protect,

include nonrepudiation, message integrity, and access restrictions.

18. D. The backup method is not an important factor to discuss with end users regarding email retention. The details of an email retention policy may need to be shared with affected subjects, which may include privacy implications, how long the messages are maintained (i.e., length of retainer), and for what purposes the messages can be used (such as auditing or violation investigations).
19. D. Static IP addressing is not an implication of multilayer protocols; it is a feature of the IP protocol when an address is defined on the local system rather than being dynamically assigned by DHCP. Multilayer protocols include the risk of VLAN hopping, multiple encapsulation, and filter evasion using tunneling.
20. B. A permanent virtual circuit (PVC) can be described as a logical circuit that always exists and is waiting for the customer to send data. Software-defined networking (SDN) is a unique approach to network operation, design, and management. SDN aims at separating the infrastructure layer (hardware and hardware-based settings) from the control layer (network services of data transmission management). A virtual private network (VPN) is a communication channel between two entities across an intermediary untrusted network. A switched virtual circuit (SVC) has to be created each time it is needed using the best paths currently available before it can be used and then disassembled after the transmission is complete.

Chapter 13: Managing Identity and Authentication

1. A. Upon implementing a cloud-based federation for identity sharing, individuals will typically use their existing normal account credentials to log in. This is facilitated by the federation service, which allows for the secure sharing of identities across different systems and providers. The use of an account provided by the cloud-based federation or a hybrid identity management approach is not necessary for the user's perspective, as these are backend solutions that enable the federation to function. Single-sign on is a related concept where a user logs in once and gains access to multiple systems without being prompted to log in again for each one, but it is a feature or capability that results from federation rather than the type of account used for login.
2. A. A primary goal when controlling access to assets is to protect against losses, including any loss of confidentiality, loss of availability, or loss of integrity. Subjects authenticate on a system, but objects do not authenticate. Subjects access objects, but objects do not access subjects. Identification and authentication are important as the first step in access control, but much more is needed to protect assets.
3. C. The subject is active and is always the entity that receives information about, or data from, the object. A subject can be a user, a program, a process, a file, a computer, a database, and so on. The object is always the entity that provides or hosts information or data. The roles of subject and object can switch while two entities communicate to accomplish a task.
4. D. NIST SP 800-63B recommends users only be required to change their password if their current password is compromised. They do not recommend that users be required to change their password regularly at any interval.
5. B. Password history can prevent users from rotating between two passwords. It remembers previously used passwords. Password complexity and password length help ensure that

users create strong passwords. Password age ensures that users change their password regularly.

6. B. A passphrase is a long string of characters that is easy to remember, such as IP@$$edTheCISSPEx@m. It is not short and typically includes at least three sets of character types. It is strong and complex, making it difficult to crack.
7. A. A synchronous authenticator generates and displays one-time passwords that are synchronized with an authentication server. An asynchronous token uses a challenge-response process to generate the one-time password. Smartcards do not generate one-time passwords, and common access cards are a version of a smartcard that includes a picture of the user.
8. C. The point at which the biometric false rejection rate and the false acceptance rate are equal is the crossover error rate (CER). It does not indicate that sensitivity is too high or too low. A lower CER indicates a more accurate biometric device, and a higher CER indicates a less accurate device.
9. A. A false rejection, sometimes called a false negative authentication or a Type I error, occurs when an authentication system doesn't recognize a valid subject (Sally in this example). A false acceptance, sometimes called a false positive authentication or a Type II error, occurs when an authentication system incorrectly recognizes an invalid subject. Crossover errors and equal errors aren't valid terms related to biometrics. However, the crossover error rate (also called equal error rate) compares the false rejection rate to the false acceptance rate and provides an accuracy measurement for a biometric system.
10. C. An authenticator app on a smartphone or tablet device is the best solution. SMS has vulnerabilities, and NIST has deprecated its use for two-factor authentication. Biometric authentication methods, such as fingerprint scans, provide strong authentication. However, purchasing biometric readers for each employee's home would be expensive. A PIN is in the something you know factor of authentication, so it doesn't provide two-factor authentication when used with a password.

11. B. Physical biometric methods such as fingerprints and iris scans provide authentication for subjects. An account ID provides identification. An authenticator is something you have, and it creates one-time passwords, but it is not related to a person's physical characteristics. A personal identification number (PIN) is something you know.

12. B, C, D. Ridges, bifurcations, and whorls are fingerprint minutiae. Ridges are the lines in a fingerprint. Some ridges abruptly end, and some ridges bifurcate or fork into branch ridges. Whorls are a series of circles. Palm scans measure vein patterns in a palm.

13. A. Fingerprints can be counterfeited or duplicated. It is not possible to change fingerprints. Users will always have a finger available (except for major medical events). It usually takes less than a minute for registration of a fingerprint.

14. A, D. Accurate identification and authentication are required to ensure logs accurately support accountability. Logs record events, including who took an action, but without accurate identification and authentication, the logs can't be relied on. Authorization grants access to resources after proper authentication. Auditing occurs after logs are created, but identification and authentication must occur first.

15. D. The best choice is to define a new role for Linux administrators and assign privileges based on the role definition. Linux systems do not have an Administrators group or a sudo group. However, you can grant root account access to users by adding them to the sudoers file. There isn't a sudo password. Instead, users execute root-level commands in the context of their own account, and their own password or if configured, the root user's password. Note that Chapter 14, “Controlling and Monitoring Access,” discusses sudo (and minimizing its use) in the context of privilege escalation.

16. C. The most likely reason (of the provided options) is to prevent sabotage. If the user's account remains enabled, the user may log on later and cause damage. Disabling the account doesn't remove the account or remove assigned privileges. Disabling an account doesn't encrypt any data, but it does retain encryption

keys that supervisors can use to decrypt any data encrypted by the user.

17. C. The most appropriate action to take when an employee leaves an organization is to disable their account. This action immediately prevents any further access to the organization's systems and data while preserving the account's data and audit trail. This is essential for any necessary follow-up investigations or in cases where access may need to be temporarily reinstated, for example, if the employee returns to the organization or if there are disputes regarding their work that need to be resolved post-departure. Deleting their account would limit the potential to audit the account's history, which could be necessary for future reference. Forcing them to change their password would allow them to retain access to their account once they have left, as they would know the new password. Taking no action for a period of time leaves unnecessary security risks, as the departing employee would still have access to the system.
18. D. It's appropriate to disable an account when an employee takes a leave of absence of 30 days or more. The account should not be deleted because the employee is expected to return after the leave of absence. If the password is reset, someone could still log on. If nothing is done to the account, someone else may access it and impersonate the employee.
19. C. Account access reviews can detect security issues for service accounts such as the sa (short for system administrator) account in Microsoft SQL Server systems. Reviews can ensure that service account passwords are strong and changed often. The other options suggest removing, disabling, or deleting the sa account, but doing so is likely to affect the database server's performance. Account deprovisioning ensures accounts are removed when they are no longer needed. Disabling an account ensures it isn't used, and account revocation deletes the account.
20. D. A periodic account access review can discover when users have more privileges than they need and could have been used to discover that this employee had permissions from several positions. Strong authentication methods (including multifactor authentication methods) would not have prevented the

problems in this scenario. Logging records what happened, but it doesn't prevent events.

Chapter 14: Controlling and Monitoring Access

1. B. The implicit deny principle ensures that access to an object is denied unless access has been expressly allowed (or explicitly granted) to a subject. It does not allow all actions that are not denied, and it doesn't require all actions to be denied.
2. B. An access control matrix includes multiple objects and subjects. It identifies access granted to subjects (such as users) to objects (such as files). A single list of subjects for any specific object within an access control matrix is an access control list. A federation refers to a group of companies that share a federated identity management (FIM) system for single sign-on (SSO). Creeping privileges refers to excessive privileges a subject gathers over time.
3. B. A discretionary access control model allows the owner (or data custodian) of a resource to grant permissions at the owner's discretion. The other answers (MAC, RBAC, and rule-based access control) are nondiscretionary models.
4. A. The DAC model allows the owner of data to modify permissions on the data. In the DAC model, objects have owners, and the owners can grant or deny access to objects that they own. The MAC model uses labels to assign access based on a user's need to know and organization policies. A rule-based access control model uses rules to grant or block access. A risk-based access control model examines the environment, the situation, and policies coded in software to determine access.
5. D. A role-based access control (RBAC) model can group users into roles based on the organization's hierarchy, and it is a nondiscretionary access control model. A nondiscretionary access control model uses a central authority to determine which objects that subjects can access. In contrast, a discretionary access control (DAC) model allows users to grant or reject access to any objects they own. An ACL is an example of a rule-based access control model that uses rules, not roles.

6. A. The role-based access control (RBAC) model is based on role or group membership, and users can be members of multiple groups. Users are not limited to only a single role. RBAC models are based on the hierarchy of an organization, so they are hierarchy-based. The mandatory access control (MAC) model uses assigned labels to identify access.
7. D. A rule-based access control model uses global rules applied to all users and other subjects equally. It does not apply rules locally or to individual users.
8. B. The ABAC model is commonly used in SDNs. None of the other answers are normally used in SDNs. The MAC model uses labels to define access, and the RBAC model uses groups. In the DAC model, the owner grants access to others.
9. B. In a hierarchical environment, the various classification labels are assigned in an ordered structure from low security to high security. The mandatory access control (MAC) model supports three environments: hierarchical, compartmentalized, and hybrid. A compartmentalized environment ignores the levels and instead only allows access for individual compartments on any level. A hybrid environment is a combination of a hierarchical and compartmentalized environment. A MAC model doesn't use a centralized environment.
10. B. The MAC model uses labels to identify the upper and lower bounds of classification levels, and these define the level of access for subjects. MAC is a nondiscretionary access control model that uses labels. However, not all nondiscretionary access control models use labels. DAC and ABAC models do not use labels.
11. C. Mandatory access control (MAC) models rely on the use of labels for subjects and objects. They look similar to a lattice when drawn, so the MAC model is often referred to as a lattice-based model. None of the other answers use labels. Discretionary access control (DAC) models allow an owner of an object to control access to the object. Nondiscretionary access controls have centralized management, such as a rule-based access control model deployed on a firewall. Role-based access

control (RBAC) models define a subject's access based on job-related roles.

12. A. A risk-based access control model can require users to authenticate with multifactor authentication. None of the other access control models listed can evaluate how a user has logged on. A MAC model uses labels to grant access. An RBAC model grants access based on job roles or groups. In a DAC model, the owner grants access to resources.

13. A. A risk-based access control model evaluates the environment and the situation and then makes access decisions based on coded policies. A MAC model grants access using labels. An RBAC model uses a well-defined collection of named job roles for access control. Administrators grant each job role with the privileges they need to perform their jobs. An ABAC model uses attributes to grant access and is often used in software-defined networks (SDNs).

14. A. OpenID Connect (OIDC) uses a JavaScript Object Notation (JSON) Web Token (JWT) that provides both authentication and profile information for internet-based single sign-on (SSO). None of the other options use tokens. OIDC is built on the OAuth 2.0 framework. TLS is a transport layer protocol that does not provide single sign-on.

15. D. Configuring a central computer to synchronize its time with an external NTP server and all other systems to synchronize their time with the NTP will likely solve the problem and is the best choice of the available options. Kerberos requires computer times to be within 5 minutes of each other and the scenario, along with the available options, suggested the user's computer is not synchronized with the Kerberos server. Kerberos uses AES. However, because a user successfully logs on to one computer, it indicates Kerberos is working, and AES is installed. NAC checks a system's health after the user authenticates. NAC doesn't prevent a user from logging on. Some federated systems use SAML, but Kerberos doesn't require SAML.

16. C. The primary purpose of Kerberos is authentication, since it allows users to prove their identity. It also provides a measure of confidentiality and integrity using symmetric key encryption,

but these are not the primary purpose. Kerberos does not include logging capabilities, so it does not provide accountability.

17. B. The network access server is the client within a RADIUS architecture. The RADIUS server is the authentication server, and it provides authentication, authorization, and accounting (AAA) services. The network access server might have a host firewall enabled, but that isn't the primary function.
18. B. The best choice is to give the administrator the root password. The administrator would enter it manually when running commands that need elevated privileges. Sudo access would allow the user to run commands requiring root-level privileges, under the context of the user account. If an attacker compromised the user account, the attacker could run the elevated commands with sudo. Linux systems don't have an administrator group or a LocalSystem account.
19. D. NTLM is known to be susceptible to pass-the-hash attacks, and this scenario describes a pass-the-hash attack. Kerberos attacks attempt to manipulate tickets, such as in pass the ticket and golden ticket attacks, but these are not NTLM attacks. A rainbow table attack uses a rainbow table in an offline brute-force attack.
20. C. Attackers can create golden tickets after successfully exploiting Kerberos and obtaining the Kerberos service account (KRBTGT). Golden tickets are not associated with Remote Authentication Dial-in User Service (RADIUS), Security Assertion Markup Language (SAML), or OpenID Connect (OIDC).

Chapter 15: Security Assessment and Testing

1. A. Nmap is a network discovery scanning tool that reports the open ports on a remote system and the firewall status of those ports. Nessus is a network vulnerability scanning tool. Metasploit is an exploitation framework used in penetration testing. `lsof` is a Linux command used to list open files on a system.
2. D. Only open ports represent potentially significant security risks. Ports 80 and 443 are expected to be open on a web server. Port 1433 is a database port and should never be exposed to an external network. Port 22 is used for the Secure Shell protocol (SSH), and the filtered status indicates that Nmap can't determine whether it is open or closed. This situation does require further investigation, but it is not as alarming as a definitely exposed database server port.
3. C. The sensitivity of information stored on the system, difficulty of performing the test, and likelihood of an attacker targeting the system are all valid considerations when planning a security testing schedule. The desire to experiment with new testing tools should not influence the production testing schedule.
4. C. Security assessments include many types of tests designed to identify vulnerabilities, and the assessment report normally includes recommendations for mitigation. The assessment does not, however, include actual mitigation of those vulnerabilities.
5. A. Security assessment reports should be addressed to the organization's management. For this reason, they should be written in plain English and avoid technical jargon.
6. C. Vulnerability scanners are used to test a system for known security vulnerabilities and weaknesses. They are not active detection tools for intrusion, they offer no form of enticement, and they do not configure system security. In addition to testing

a system for security weaknesses, they produce evaluation reports and make recommendations.

7. B. The server is likely running a website on port 80. Using a web browser to access the site may provide important information about the site's purpose.
8. B. The SSH protocol uses port 22 to accept administrative connections to a server.
9. D. Authenticated scans can read configuration information from the target system and reduce the instances of false positive and false negative reports.
10. C. The TCP SYN scan sends a SYN packet and receives a SYN ACK packet in response, but it does not send the final ACK required to complete the three-way handshake.
11. D. SQL injection attacks are web vulnerabilities, and Matthew would be best served by a web vulnerability scanner. A network vulnerability scanner might also pick up this vulnerability, but the web vulnerability scanner is specifically designed for the task and more likely to be successful.
12. C. The scenario does not provide us with enough information to determine whether this exercise involved red team, blue team, or purple team tactics, and in fact, those exercises typically involve live access to systems. Tabletop exercises, on the other hand, are designed to walk teams through a scenario, and that is what Tina is doing in this instance.
13. B. Metasploit is an automated exploit tool that allows attackers to easily execute common attack techniques. Nmap is a port scanning tool. Nessus is a network vulnerability scanner, and Nikto is a web application scanner. While these other tools might identify potential vulnerabilities, they do not go as far as to exploit them.
14. C. Mutation fuzzing uses bit flipping and other techniques to slightly modify previous inputs to a program in an attempt to detect software flaws.
15. A. Misuse case testing identifies known ways that an attacker might exploit a system and tests explicitly to see if those attacks

are possible in the proposed code.

16. B. User interface testing includes assessments of both graphical user interfaces (GUIs) and command-line interfaces (CLIs) for a software program.
17. B. During a white-box penetration test, the testers have access to detailed configuration information about the system being tested.
18. B. Unencrypted HTTP communications take place over TCP port 80 by default.
19. B. There are only two types of SOC report: Type I and Type II. Both reports provide information on the suitability of the design of security controls. Only a Type II report also provides an opinion on the operating effectiveness of those controls over an extended period of time.
20. B. The backup verification process ensures that backups are running properly and thus meeting the organization's data protection objectives.

Chapter 16: Managing Security Operations

1. C. The need-to-know policy operates on the basis that any given system user should be granted access only to portions of sensitive information or materials necessary to perform some task. The principle of least privilege ensures personnel are granted only the permissions they need to perform their job and no more. Segregation of duties ensures that no single person has total control over a critical function or system. There isn't a standard principle called “as-needed basis.”
2. C. Need-to-know is the requirement to have access to, knowledge about, or possession of data to perform specific work tasks, but no more. The principle of least privilege includes both rights and permissions, but the term principle of least permission is not valid within IT security. Segregation of duties (SoD) ensures that a single person doesn't control all the elements of a process. A segregation of duties policy ensures that no single person has total control over a critical function. A job rotation policy requires employees to rotate to different jobs periodically
3. C. An organization applies the least privilege principle to ensure employees receive only the access they need to complete their job responsibilities. Need-to-know refers to permissions only, while privileges include both rights and permissions. A mandatory vacation policy requires employees to take a vacation in one- or two-week increments. An SLA identifies performance expectations and can include monetary penalties.
4. D. Microsoft domains include a privileged account management solution that grants administrators elevated privileges when they need them, but restricts the access using a time-limited ticket. The principle of least privilege includes both rights and permissions, but the term principle of least permission is not valid within IT security. Segregation of duties ensures that a single person doesn't control all the elements of a process or a critical function. Need-to-know is the requirement to have

access to, knowledge about, or possession of data to perform specific work tasks, but no more.

5. D. The default level of access, should be no access. The principle of least privilege dictates that users should only be granted the level of access they need for their job, and the question doesn't indicate that new users need any access to the database. Read access, modify access, and full access grants users some level of access, which violates the principle of least privilege.
6. A. Each account should be given only the rights and permissions needed to perform their job when following the least privilege policy. New employees would not need full rights and permissions to a server. Employees will need some rights and permissions in order to do their job. Regular user accounts should not be added to the Administrators group.
7. C. Segregation of duties ensures that no single entity can perform all of the tasks for a job or function. A job rotation policy moves employees to different jobs periodically. A mandatory vacation policy requires employees to take vacations. A least privilege policy ensures users have only the privileges they need, and no more.
8. A. A job rotation policy has employees rotate jobs or job responsibilities and can help detect collusion and fraud. A segregation of duties policy ensures that a single person doesn't control all elements of a specific function. Mandatory vacation policies ensure that employees take an extended time away from their job, requiring someone else to perform their job responsibilities, which increases the likelihood of discovering fraud. Least privilege ensures that users have only the permissions they need to perform their job and no more.
9. B. Mandatory vacation policies help detect fraud. They require employees to take an extended time away from their job, requiring someone else to perform their job responsibilities, which increases the likelihood of discovering fraud. It does not rotate job responsibilities. While mandatory vacations might help employees reduce their overall stress levels and increase productivity, these are not the primary reasons for mandatory vacation policies.

10. C. A service-level agreement (SLA) can provide monetary penalties if a third-party provider doesn't meet its contractual requirements. Neither a memorandum of understanding (MOU) nor an interconnection security agreement (ISA) includes monetary penalties. Segregation of duties (SoD) is sometimes shortened to SED, but this is unrelated to third-party relationships.
11. A. The IaaS service model provides an organization with the most control compared to the other models, and this model requires the organization to perform all maintenance on operating systems and applications. The SaaS model gives the organization the least control, and the cloud service provider (CSP) is responsible for all maintenance. The PaaS model splits control and maintenance responsibilities between the CSP and the organization.
12. C. The SaaS service model provides services such as email available via a web browser. IaaS provides the infrastructure (such as servers), and PaaS provides a platform (such as an operating system and application installed on a server). Public is a deployment method, not a service model.
13. A. When images are used to deploy systems, the systems start with a common baseline, which is important for configuration management. Images don't necessarily improve the evaluation, approval, deployment, and audits of patches to systems within the network. While images can include current patches to reduce their vulnerabilities, this is because the image provides a baseline. Change management provides documentation for changes.
14. C. An effective change management program helps prevent outages from unauthorized changes. Vulnerability management helps detect weaknesses but wouldn't block the problems from this modification. Patch management ensures systems are kept up-to-date. Blocking scripts removes automation, which would increase the overall workload.
15. B, C, D. Change management processes include requesting a change, creating a rollback plan for the change, and

documenting the change. Changes should not be implemented immediately without evaluating the change.

16. C. Change management aims to ensure that any change does not result in unintended outages or reduce security. Change management doesn't affect personnel safety. A change management plan will commonly include a rollback plan, but that isn't a specific goal of the program. Change management doesn't perform any type of auditing.
17. D. An effective patch management program evaluates and tests patches before deploying them and would have prevented this problem. Approving all patches would not prevent this problem because the same patch would be deployed. Systems should be audited after deploying patches, not to test for the impact of new patches.
18. A. A patch management system ensures that systems have required patches. In addition to deploying patches, it would check the systems to verify they accepted the patches. There is no such thing as a patch scanner. A penetration test will attempt to exploit a vulnerability, but it can be intrusive and cause an outage, so it isn't appropriate in this scenario. A fuzz tester sends random data to a system to check for vulnerabilities but doesn't test for patches.
19. B. Vulnerability scanners are used to check systems for known issues and are part of an overall vulnerability management program. Versioning is used to track software versions and is unrelated to detecting vulnerabilities. Security audits and reviews help ensure that an organization is following its policies but wouldn't directly check systems for vulnerabilities.
20. D. A vulnerability scan will list or enumerate all known security risks within a system. None of the other options will list security risks within a system. Configuration management systems check and modify configuration settings. Patch management systems can deploy patches and verify patches are deployed, but they don't check for all known security risks. Hardware inventories only verify the hardware is still present.

Chapter 17: Preventing and Responding to Incidents

1. B, C, D. Detection, reporting, and lessons learned are valid incident management steps. Prevention is done before an incident. Creating backups can help recovering systems, but it isn't one of the incident management steps. The seven steps (in order) are detection, response, mitigation, reporting, recovery, remediation, and lessons learned.
2. A. The next step is to isolate the computer from the network as part of the mitigation phase. He might look at other computers later, but he should try to mitigate the problem first. Similarly, he might run an antivirus scan, but later. The lessons learned phase is last and will analyze an incident to determine the cause.
3. D. The first step is detection. The seven steps (in order) are detection, response, mitigation, reporting, recovery, remediation, and lessons learned.
4. A, C, D. The three basic security controls listed are (A) keep systems and applications up-to-date, (C) remove or disable unneeded services or protocols, and (D) use up-to-date antimalware software. SOAR technologies implement advanced methods to detect and automatically respond to incidents. It's appropriate to place a network firewall at the border (between the Internet and the internal network), but web application firewall (WAF) should only filter traffic going to a web server.
5. B. Audit trails provide documentation on what happened, when it happened, and who did it. IT personnel create audit trails by examining logs. Authentication of individuals is also needed to ensure the audit trails provide proof of identities listed in the logs. Identification occurs when an individual claims an identity, but identification without authentication doesn't provide accountability. Authorization grants individuals access to resources based on their proven identity. Confidentiality ensures that unauthorized entities can't access sensitive data and is unrelated to this question.

6. B. The first step should be to copy existing logs to a different drive so that they are not lost. If you enable rollover logging, you are configuring the logs to overwrite old entries. It's not necessary to review the logs before copying them. If you delete the oldest log entries first, you may delete valuable data.
7. A. Fraggle is a denial-of-service (DoS) that uses UDP. Other attacks, such as a SYN flood attack, use TCP. A Smurf attack is similar to a Fraggle attack, but it uses ICMP. SOAR is a group of technologies that provides automated responses to common attacks; SOAR is not a protocol.
8. A. A zero-day exploit is an attack that exploits a vulnerability that doesn't have a patch or fix. A newly discovered vulnerability is only a vulnerability until someone tries to exploit it. Attacks on unpatched systems aren't zero-day exploits. A virus is a type of malware that delivers its payload after a user launches an application.
9. C. This is a false positive. The IPS falsely identified normal web traffic as an attack and blocked it. A false negative occurs when a system doesn't detect an actual attack. A honeynet is a group of honeypots used to lure attackers. Sandboxing provides an isolated environment for testing and is unrelated to this question.
10. D. An anomaly-based IDS requires a baseline, and it then monitors traffic for any anomalies or changes when compared to the baseline. It's also called behavior-based and heuristics-based. Pattern-based detection (also known as knowledge-based detection and signature-based detection) uses known signatures to detect attacks.
11. B. An NIDS will monitor all traffic and raise alerts when it detects suspicious traffic. An HIDS only monitors a single system. A honeynet is a network of honeypots used to lure attackers away from live networks. A network firewall filters traffic, but it doesn't raise alerts on suspicious traffic.
12. A. This describes an NIPS. It is monitoring network traffic, and it is placed inline with the traffic. An NIDS isn't placed inline

with the traffic, so it isn't the best choice. Host-based systems only monitor traffic sent to specific hosts, not network traffic.

13. D. A drawback of some HIDSs is that they interfere with a single system's normal operation by consuming too many resources. The other options refer to applications that aren't installed on user systems.
14. B. An IDS is most likely to connect to a switch port configured as a mirrored port. An IPS is placed inline with traffic, so it is placed before the switch. A honeypot doesn't need to see all traffic going through a switch. A sandbox is an isolated area often used for testing and would not need all traffic from a switch.
15. B. A false negative occurs when there is an attack, but the NIDS doesn't detect it and does not raise an alarm. In contrast, a false positive occurs when an NIDS incorrectly raises an alarm, even though there isn't an attack. The attack may be a UDP-based Fraggle attack or an ICMP-based Smurf attack, but the attack is real, and if the IDS doesn't detect it, it is a false negative.
16. B. An anomaly-based IDS (also known as a behavior-based IDS) can detect new security threats. A signature-based IDS only detects attacks from known threats. An active IDS identifies the response after a threat is detected. A network-based IDS can be both signature-based and anomaly-based.
17. B. A security information and event management (SIEM) system is a centralized application that monitors multiple systems. Security orchestration, automation, and response (SOAR) is a group of technologies that provide automated responses to common attacks. A host-based intrusion detection system (HIDS) is decentralized because it is on one system only. A threat feed is a stream of data on current threats.
18. D. A network-based data loss prevention (DLP) system monitors outgoing traffic (egress monitoring) and can thwart data exfiltration attempts. Network-based intrusion detection systems (NIDSs) and intrusion protection systems (IPSs) primarily monitor incoming traffic for threats. Firewalls can block traffic or allow traffic based on rules in an access control

list (ACL), but they can't detect unauthorized data exfiltration attacks.

19. A. Threat hunting is the process of actively searching for infections or attacks within a network. Threat intelligence refers to the actionable intelligence created after analyzing incoming data, such as threat feeds. Threat hunters use threat intelligence to search for specific threats. Additionally, they may use a kill chain model to mitigate these threats. Artificial intelligence (AI) refers to actions by a machine, but the scenario indicates administrators are doing the work.

20. A. Security orchestration, automation, and response (SOAR) technologies provide automated responses to common attacks, reducing an administrator's workload. A security information and event management (SIEM) system is a centralized application that monitors log entries from multiple sources. A network-based intrusion detection system (NIDS) raises alerts. A data loss prevention (DLP) system helps with egress monitoring and is unrelated to this question.

Chapter 18: Disaster Recovery Planning

1. C. Once a disaster interrupts the business operations, the goal of DRP is to restore regular business activity as quickly as possible. Thus, disaster recovery planning picks up where business continuity planning leaves off. Preventing business interruption is the goal of business continuity, not disaster recovery programs. While disaster recovery programs are involved in setting up temporary operations and minimizing the impact of disasters, this is not their end goal.
2. C. The recovery point objective (RPO) specifies the maximum amount of data that may be lost during a disaster and should be used to guide backup strategies. The maximum tolerable downtime (MTD) and recovery time objective (RTO) are related to the duration of an outage, rather than the amount of data lost. The mean time between failures (MTBF) is related to the frequency of failure events.
3. D. The lessons learned session captures discoveries made during the disaster recovery process and facilitates continuous improvement. It may identify deficiencies in training and awareness or the BIA.
4. B. Redundant arrays of inexpensive disks (RAID) are a fault tolerance control that allow an organization's storage service to withstand the loss of one or more individual disks. Load balancing, clustering, and HA pairs are all fault tolerance services designed for server compute capacity, not storage.
5. C. Cloud computing services provide an excellent location for backup storage because they are accessible from any location. The primary data center is a poor choice, as it may be damaged during a disaster. A field office is reasonable, but it is in a specific location and is not as flexible as a cloud-based approach. The IT manager's home is a poor choice, as the IT manager may leave the organization or may not have appropriate environmental and physical security controls in place.

6. A, B, D. The only incorrect statement here is that business continuity planning picks up where disaster recovery planning leaves off. In fact, the opposite is true: Disaster recovery planning picks up where business continuity planning leaves off. The other three statements are all accurate reflections of the role of business continuity planning and disaster recovery planning. Business continuity planning is focused on keeping business functions uninterrupted when a disaster strikes. Organizations can choose whether to develop business continuity planning or disaster recovery planning plans. Disaster recovery planning guides an organization through recovery of normal operations at the primary facility.
7. B. The term *100-year floodplain* is used to describe an area where flooding is expected once every 100 years. It is, however, more mathematically correct to say that this label indicates a 1 percent probability of flooding in any given year.
8. D. When you use remote mirroring, an exact copy of the database is maintained at an alternative location. You keep the remote copy up-to-date by executing all transactions on both the primary and remote sites at the same time. Electronic vaulting follows a similar process of storing all data at the remote location, but it does not do so in real time. Transaction logging and remote journaling options send logs, rather than full data replicas, to the remote location.
9. C. All of these are good practices that could help improve the quality of service that Bryn provides from her website. Installing dual power supplies or deploying RAID arrays could reduce the likelihood of a server failure, but these measures only protect against a single risk each. Deploying multiple servers behind a load balancer is the best option because it protects against any type of risk that would cause a server failure. Backups are an important control for recovering operations after a disaster, and different backup strategies could indeed alter the RTO, but it is even better if Bryn can design a web architecture that lowers the risk of the outage occurring in the first place.
10. B. During the business impact analysis phase, you must identify the business priorities of your organization to assist with the

allocation of BCP resources. You can use this same information to drive the DRP business unit prioritization.

11. C. The cold site contains none of the equipment necessary to restore operations. All of the equipment must be brought in and configured and data must be restored to it before operations can commence. This often takes weeks, but cold sites also have the lowest cost to implement. Hot sites, warm sites, and mobile sites all have quicker recovery times.
12. C. Uninterruptible power supplies (UPS) provide a battery-backed source of power that is capable of preserving operations in the event of brief power outages. Generators take a significant amount of time to start and are more suitable for longer-term outages. Dual-power supplies protect against power supply failures and not power outages. Redundant network links are a network continuity control and do not provide power.
13. D. Warm sites and hot sites both contain workstations, servers, and the communications circuits necessary to achieve operational status. The main difference between the two alternatives is the fact that hot sites contain near-real-time copies of the operational data, and warm sites require the restoration of data from backup.
14. D. The parallel test involves relocating personnel to the alternate recovery site and implementing site activation procedures. Read-throughs, walk-throughs, and simulations are all test types that do not involve actually activating the alternate site.
15. A. The executive summary provides a high-level view of the entire organization's disaster recovery efforts. This document is useful for the managers and leaders of the firm as well as public relations personnel who need a nontechnical perspective on this complex effort.
16. D. Software escrow agreements place the application source code in the hands of an independent third party, thus providing firms with a “safety net” in the event a developer goes out of business or fails to honor the terms of a service agreement.
17. A. Differential backups involve always storing copies of all files modified since the most recent full backup regardless of any

incremental or differential backups created during the intervening time period.

18. B. People should always be your highest priority in business continuity planning. As a life safety system, fire suppression systems should always receive high prioritization.
19. A. Any backup strategy must include full backups at some point in the process. If a combination of full and differential backups is used, a maximum of two backups must be restored. If a combination of full and incremental backups is chosen, the number of required restorations may be large.
20. B. Parallel tests involve moving personnel to the recovery site and gearing up operations, but responsibility for conducting day-to-day operations of the business remains at the primary operations center.

Chapter 19: Investigations and Ethics

1. C. A crime is any violation of a law or regulation. The violation stipulation defines the action as a crime. It is a computer crime if the violation involves a computer either as the target or as a tool. Computer crimes may not be defined in an organization's policy, as crimes are only designed in law. Illegal attacks are indeed crimes, but this is too narrow of a definition. The failure to practice due diligence may be a liability but, in most cases, is not a criminal action.
2. B. A military and intelligence attack is targeted at the classified data that resides on the system. To the attacker, the value of the information justifies the risk associated with such an attack. The information extracted from this type of attack is often used to plan subsequent attacks.
3. A. The code of ethics does not require that you protect your colleagues.
4. B. A financial attack focuses primarily on obtaining services and funds illegally. Accessing services that you have not purchased is an example of obtaining services illegally. Transferring funds from an unapproved source is obtaining funds illegally, as is leasing out a botnet for use in DDoS attacks. Disclosing confidential information is not necessarily financially motivated.
5. B. A terrorist attack is launched to interfere with a way of life by creating an atmosphere of fear. A computer terrorist attack can reach this goal by reducing the ability to respond to a simultaneous physical attack. While terrorists may engage in other actions, such as altering information, stealing data, or transferring funds, as part of their attacks, these items alone are not indicators of terrorist activity.
6. D. Any action that can harm a person or organization, either directly or through embarrassment, would be a valid goal of a grudge attack. The purpose of such an attack is to “get back” at someone.

7. A, C. Thrill attacks have no reward other than providing a boost to pride and ego. The thrill of launching the attack comes from the act of participating in the attack (and not getting caught).
8. C. Although the other options have some merit in individual cases, the most important rule is to never modify, or taint, evidence. If you modify evidence, it becomes inadmissible in court.
9. D. The most compelling reason for not removing power from a machine is that you will lose the contents of memory. Carefully consider the pros and cons of removing power. After all is considered, it may be the best choice.
10. C. Written documents brought into court to prove the facts of a case are referred to as documentary evidence. The best evidence rule states that when a document is used as evidence in a court proceeding, the original document must be introduced. The parol evidence rule states that when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement. Testimonial evidence is evidence consisting of the testimony of a witness, either verbal testimony in court or written testimony in a recorded deposition.
11. C. Criminal investigations may result in the imprisonment of individuals and, therefore, have the highest standard of evidence to protect the rights of the accused.
12. B. Root cause analysis seeks to identify the reason that an operational issue occurred. The root cause analysis often highlights issues that require remediation to prevent similar incidents in the future. Forensic analysis is used to obtain evidence from digital systems. Network traffic analysis is an example of a forensic analysis category. Fagan inspection is a software testing technique.
13. A. Preservation ensures that potentially discoverable information is protected against alteration or deletion. Production places the information into a format that may be shared with others and delivers it to other parties, such as

opposing counsel. Processing screens the collected information to perform a “rough cut” of irrelevant information, reducing the amount of information requiring detailed screening. Presentation displays the information to witnesses, the court, and other parties.

14. B. Server logs are an example of documentary evidence. Gary may ask that they be introduced in court and will then be asked to offer testimonial evidence about how he collected and preserved the evidence. This testimonial evidence authenticates the documentary evidence.
15. B. In this case, you need a search warrant to confiscate equipment without giving the suspect time to destroy evidence. If the suspect worked for your organization and you had all employees sign consent agreements, you could simply confiscate the equipment.
16. A. Log files contain a large volume of generally useless information. However, when you are trying to track down a problem or an incident, they can be invaluable. Even if an incident is discovered as it is happening, it may have been preceded by other incidents. Log files provide valuable clues and should be protected and archived, often by forwarding log entries to a centralized log management system.
17. D. Review examines the information resulting from the Processing phase to determine what information is responsive to the request and remove any information protected by attorney-client privilege. Identification locates the information that may be responsive to a discovery request when the organization believes that litigation is likely. Collection gathers the relevant information centrally for use in the eDiscovery process. Processing screens the collected information to perform a “rough cut” of irrelevant information, reducing the amount of information requiring detailed screening.
18. D. Ethics are simply rules of personal behavior. Many professional organizations establish formal codes of ethics to govern their members, but ethics are personal rules individuals use to guide their lives.

19. B. The second canon of the ISC2 Code of Ethics states how a CISSP should act, which is honorably, honestly, justly, responsibly, and legally.
20. B. RFC 1087 does not specifically address the statements in A, C, or D. Although each type of activity listed is unacceptable, only "actions that compromise the privacy of users" are explicitly identified in RFC 1087.

Chapter 20: Software Development Security

1. A. The three elements of the DevOps model are software development, quality assurance, and IT operations. Information security is only introduced in the DevSecOps model.
2. B. Input validation ensures that the input provided by users matches the design parameters. Polyinstantiation includes additional records in a database for presentation to users with differing security levels as a defense against inference attacks. Contamination is the mixing of data from a higher classification level and/or need-to-know requirement with data from a lower classification level and/or need-to-know requirement. Screening is a generic term and does not represent any specific security technique in this context.
3. C. Request control provides users with a framework to request changes and developers with the opportunity to prioritize those requests. Configuration control ensures that changes to software versions are made in accordance with the change and configuration management policies. Request control provides an organized framework for users to request modifications. Change auditing is used to ensure that the production environment is consistent with the change accounting records.
4. C. In a fail-secure state, the system remains in a high level of security until an administrator intervenes. In a fail-open state, the system defaults to a low level of security, disabling controls until the failure is resolved. Failure mitigation seeks to reduce the impact of a failure. Fail-clear is not a valid approach.
5. B. The iterative waterfall model uses a seven-stage approach to software development and includes a feedback loop that allows development to return to the previous phase to correct defects discovered during the subsequent phase.
6. B. The activities of threat assessment, threat modeling, and security requirements are all part of the Design function under SAMM.

7. C. Foreign keys are used to enforce referential integrity constraints between tables that participate in a relationship. Candidate keys are sets of fields that may potentially serve as the primary key, the key used to uniquely identify database records. Alternate keys are candidate keys that are not selected as the primary key.
8. D. In this case, the process the database user is taking advantage of is aggregation. Aggregation attacks involve the use of specialized database functions to combine information from a large number of database records to reveal information that may be more sensitive than the information in individual records would reveal. Inference attacks use deductive reasoning to reach conclusions from existing data. Contamination is the mixing of data from a higher classification level and/or need-to-know requirement with data from a lower classification level and/or need-to-know requirement. Polyinstantiation is the creation of different database records for users of differing security levels.
9. C. Polyinstantiation allows the insertion of multiple records that appear to have the same primary key values into a database at different classification levels. Aggregation attacks involve the use of specialized database functions to combine information from a large number of database records to reveal information that may be more sensitive than the information in individual records would reveal. Inference attacks use deductive reasoning to reach conclusions from existing data. Manipulation is the authorized or unauthorized alteration of data in a database.
10. D. In Agile, the highest priority is to satisfy the customer through early and continuous delivery of valuable software. It is not to prioritize security over other requirements. The Agile principles also include satisfying the customer through early and continuous delivery, businesspeople and developers working together, and paying continuous attention to technical excellence.
11. C. Expert systems use a knowledge base consisting of a series of “if/then” statements to form decisions based on the previous experience of human experts.

12. D. In the Managed phase, level 4 of the SW-CMM, the organization uses quantitative measures to gain a detailed understanding of the development process.
13. B. ODBC acts as a proxy between applications and the backend DBMS. The software development life cycle (SDLC) is a model for the software development process that incorporates all necessary activities. The Payment Card Industry Data Security Standard (PCI DSS) is a regulatory framework for payment card processing. Abstraction is a software development concept that generalizes common behaviors of software objects into more abstract classes.
14. A. In order to conduct a static test, the tester must have access to the underlying source code. Black-box testing does not require access to source code. Dynamic testing is an example of black-box testing. Cross-site scripting is a specific type of vulnerability, and it may be discovered using both static and dynamic techniques, with or without access to the source code.
15. A. A Gantt chart is a type of bar chart that shows the interrelationships over time between projects and schedules. It provides a graphical illustration of a schedule that helps to plan, coordinate, and track specific tasks in a project. A PERT chart focuses on the interrelationships between tasks rather than the specific details of the schedule. Bar charts are used to present data, and Venn diagrams are used to show the relationships between sets.
16. C. Contamination is the mixing of data from a higher classification level and/or need-to-know requirement with data from a lower classification level and/or need-to-know requirement. Aggregation attacks involve the use of specialized database functions to combine information from a large number of database records to reveal information that may be more sensitive than the information in individual records would reveal. Inference attacks use deductive reasoning to reach conclusions from existing data. Polyinstantiation includes additional records in a database for presentation to users with differing security levels as a defense against inference attacks.

17. D. Tonya is purchasing the software, so it is not open-source. It is used widely in her industry, so it is not custom developed for her organization. There is no indication in the question that the software is an enterprise resource planning (ERP) system. The best answer here is commercial-off-the-shelf software (COTS).
18. C. Configuration audit is part of the configuration management process rather than the change management process. Request control, release control, and change control are all components of the change management process.
19. C. The isolation principle states that two transactions operating on the same data must be temporarily separated from each other such that one does not interfere with the other. The atomicity principle says that if any part of the transaction fails, the entire transaction must be rolled back. The consistency principle says that the database must always be in a state that complies with the database model's rules. The durability principle says that transactions committed to the database must be preserved.
20. B. The cardinality of a table refers to the number of rows in the table, while the degree of a table is the number of columns. In this case, the table has three columns (name, telephone number, and customer ID), so it has a degree of three.

Chapter 21: Malicious Code and Application Attacks

1. D. User and entity behavior analytics (UEBA) tools develop profiles of individual behavior and then monitor users for deviations from those profiles that may indicate malicious activity and/or compromised accounts. This type of tool would meet Dylan's requirements. Endpoint detection and response (EDR) tools watch for unusual endpoint behavior but do not analyze user activity. Integrity monitoring is used to identify unauthorized system/file changes. Signature detection is a malware detection technique.
2. B. All of these technologies are able to play important roles in defending against malware and other endpoint threats. User and entity behavior analysis (UEBA) looks for behavioral anomalies. Endpoint detection and response (EDR) and next generation endpoint protection (NGEP) identify and respond to malware infections. However, only managed detection and response (MDR) combines antimalware capabilities with a managed service that reduces the burden on the IT team.
3. C. If Carl has backups available, that would be his best option to recover operations. He could also pay the ransom, but this would expose his organization to legal risks and incur unnecessary costs. Rebuilding the systems from scratch would not restore his data. Installing antivirus software would be helpful in preventing future compromises, but these packages would not likely be able to decrypt the missing data.
4. A. While an advanced persistent threat (APT) may leverage any of these attacks, they are most closely associated with zero-day exploits due to the cost and complexity of the research required to discover or purchase them. Social engineering, Trojans (and other malware), and SQL injection attacks are often attempted by many different types of attackers.
5. B. Buffer overflow vulnerabilities exist when a developer does not properly validate user input to ensure that it is of an

appropriate size. Input that is too large can “overflow” a data structure to affect other data stored in the computer's memory. Time-of-check to time-of-use (TOCTTOU) attacks exploit timing differences that lead to race conditions. Cross-site scripting (XSS) attacks force the execution of malicious scripts in the user's browser. Cross-site request forgery (XSRF) attacks exploit authentication trust between browser tabs.

6. B. TOC/TOU is a type of timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request. Backdoors are code that allow those with knowledge of the back door to bypass authentication mechanisms. Buffer overflow vulnerabilities exist when a developer does not properly validate user input to ensure that it is of an appropriate size. Input that is too large can “overflow” a data structure to affect other data stored in the computer's memory. SQL injection attacks include SQL code in user input in the hopes that it will be passed to and executed by the backend database.

7. D. The `try…catch` clause is used to attempt to evaluate code contained in the try clause and then handle errors with the code located in the catch clause. The other constructs listed here (`if…then`, `case…when`, and `do…while`) are all used for control flow.

8. C. In this case, the `..` operators are the telltale giveaway that the attacker was attempting to conduct a directory traversal attack. This particular attack sought to break out of the web server's root directory and access the `/etc/passwd` file on the server. SQL injection attacks would contain SQL code in them. File upload attacks seek to upload a file to the server. Session hijacking attacks require the theft of authentication tokens or other credentials.

9. A. Logic bombs wait until certain conditions are met before delivering their malicious payloads. Worms are malicious code objects that move between systems under their own power, while viruses require some type of human intervention. Trojan horses masquerade as useful software but then carry out malicious functions after installation.

10. D. The single quote character (`'`) is used in SQL queries and must be handled carefully on web forms to protect against SQL injection attacks.
11. B. Developers of web applications should leverage parametrized queries or stored procedures to limit the application's ability to execute arbitrary code. With stored procedures, the SQL statement resides on the database server and may only be modified by database developers or administrators. With parameterized queries, the SQL statement is defined within the application and variables are bound to that statement in a safe manner.
12. C. While any malware may be leveraged for financial gain, depending upon its payload, cryptomalware is specifically designed for this purpose. It steals computing power and uses it to mine cryptocurrency. Remote access Trojans (RATs) are designed to grant attackers remote administrative access to systems. Potentially unwanted programs (PUPs) are any type of software that is initially approved by the user but then performs undesirable actions. Worms are malicious code objects that move between systems under their own power.
13. A. Cross-site scripting attacks are often successful against web applications that include reflected input. This is one of the two main categories of XSS attacks in a discussion forum posting. The script content will then be processed each time another visitor views the posting from the attacker. The injected script code can cause additional browser pop-ups leading to URLs of the attacker's choosing.
14. D. Buffer overflow attacks allow an attacker to modify the contents of a system's memory by writing beyond the space allocated for a variable.
15. A. Packets with internal source IP addresses should not be allowed to enter the network from the outside because they are likely spoofed. Packets with internal source IP addresses should be able to exit the network from the inside, and packets with external source IP addresses should be able to enter the network from the outside, as these are both normal network activity.

Packets with public IP addresses should be able to pass through the firewall in both directions, assuming that they meet other security requirements.

16. B. Cross-site scripting (XSS) attacks insert content on a website that causes viewers of that content to execute a script. Although this website is backed by a database, the threat that Bob is worried about does not affect the backend database and, therefore, is not a SQL injection attack. Buffer overflow attacks attempt to manipulate the contents of memory, and evil twin attacks are against wireless networks, not websites.
17. B, C, D. Input validation protects against a wide variety of web-based attacks, including SQL injection. Input validation typically includes checking for appropriate length, checking for known examples of malware or abusive input, and escaping metacharacters. Developers may also defend against SQL injection attacks by using stored procedures and parameterized queries. User acceptance testing verifies the proper functioning of code and is not a protection against SQL injection attacks.
18. A. SQL injection attacks allow attackers to include their own SQL commands in the commands issued by a web application to a database.
19. A. Ransomware's signature characteristic is the encryption of files using a key known only to the attacker and then demanding payment in exchange for the decryption key.
20. A. User and entity behavior analytics (UEBA) tools develop profiles of individual behavior and then monitor users for deviations from those profiles that may indicate malicious activity and/or compromised accounts. This type of tool would meet Rhonda's requirements.